

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-222360

(43)Date of publication of application : 11.08.2000

(51)Int.Cl. G06F 15/00

G06F 12/14

G06F 13/00

G06K 17/00

H04L 9/32

(21)Application number : 11-024446 (71)Applicant : MATSUSHITA ELECTRIC IND
CO LTD

(22)Date of filing : 01.02.1999 (72)Inventor : SHIBATA AKIO
TAKAYAMA HISASHI

(54) METHOD AND SYSTEM FOR AUTHENTICATION AND AUTHENTICATION PROCESSING PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To exclude any illegal access by identifying any legal access with a small calculation quantity in single sign on type authentication for permitting plural times of access by single user authentication.

SOLUTION: Secrecy information 4 is shared by a client means 1 and an authentication server means 2. The authentication server means 2 issues an authentication ticket 5 including collation information obtained by performing an irreversible arithmetic operation (f) on the secrecy information 4 (n) times. The client means 1 indicates this authentication ticket and presentation information obtained by performing an irreversible arithmetic operation (f) on the secrecy information 4 (n-k) times to a permission server means 3. The permission server means 3 performs the irreversible arithmetic operation (f) on the presented information (k) times, and checks whether or not this presented information matches the collation information. In this case, (k) is increased from 1 to (n) so that the authentication ticket 5 can be

used for the maximum (n) times of access without calculating the next presented information from the past presented information.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] An authentication server means to publish an authentication ticket, and a license server means to approve use of an authentication ticket, In an authentication system equipped with a client means to require an authentication ticket of said authentication server means, and to require use license of an authentication ticket of said license server means A client means to hold the authentication ticket whose count of effective is n (n is a positive integer), and for this to be shown, and to ask for use license, A license server means to require presentation information of said client means in response, to collate with said authentication ticket, and to approve use is provided. Said authentication ticket The authentication child is given including a ticket identifier, collating information, and the count of effective. Said collating information A predetermined irreversible operation is performed to the confidential information which said authentication server means and said client means share n times. Said presentation information in case the use count of said authentication ticket is k (k is a positive integer below n) is an authentication system characterized by performing said predetermined irreversible operation to said confidential

information n-k times.

[Claim 2] The authentication system according to claim 1 to which said authentication server means is characterized by managing user authentication information, performing a user authentication procedure between said client means, and publishing said authentication ticket.

[Claim 3] It is the authentication system according to claim 2 which said authentication server means generates a random number in a user authentication procedure, this is shown, authentication presentation information is required of said client means, and said confidential information performs said predetermined irreversible operation to connection by said user authentication information and said random number once or more, and is characterized by said authentication presentation information performing said predetermined irreversible operation to said confidential information n times.

[Claim 4] Said authentication server means generates a random number in a user authentication procedure, shows this, and requires authentication presentation information of a client means. Said authentication presentation information is as a result of [of what performed said predetermined irreversible operation to connection by said user authentication information and said random number once or more, and the random number for authentication which said client means generated] EXCLUSIVE OR operation. The authentication system according to claim 2 characterized by said confidential information being said random number for authentication counted backward from said authentication presentation information.

[Claim 5] An authentication system given in either of claims 2-4 characterized by said user authentication information being the password entered by the user.

[Claim 6] An authentication system given in either of claims 2-4 characterized by said user authentication information being the common key system cryptographic key held in secrecy.

[Claim 7] An authentication system given in either of claims 1-6 to which said authentication child is characterized by being a message authorization code.

[Claim 8] An authentication system given in either of claims 1-6 to which said authentication child is characterized by being a digital signature.

[Claim 9] An authentication system given in either of claims 1-8 to which said predetermined irreversible operation is characterized by on the other hand being a tropism hash operation.

[Claim 10] An authentication system given in either of claims 1-9 to which said authentication ticket is characterized by including a server identifier.

[Claim 11] An authentication system given in either of claims 1-10 to which said authentication ticket is characterized by including the time of the date of issue.

[Claim 12] The authentication system according to claim 11 characterized by for said authentication ticket updating the collating information on said authentication ticket, the count of effective, the time of the date of issue, a publisher identifier, and an

authentication child including a publisher identifier while said license server means carries out use license, for said collating information being updated by what performed said predetermined irreversible operation to said confidential information $n-k$ times, and said count of effective being updated by $n-k$.

[Claim 13] An authentication system given in either of claims 1-12 to which said license server means is characterized by having managed the use count of said authentication ticket, showing this, and requiring presentation information.

[Claim 14] An authentication system given in either of claims 1-12 to which said client means is characterized by having managed the use count of said authentication ticket, showing this with said authentication ticket, and asking for use license.

[Claim 15] It has said two or more license server means and the authentication ticket management tool which manages the use count of said authentication ticket. Said client means It is what has managed the use count of said authentication ticket, shows this with said authentication ticket, and asks for use license. Said authentication server means While publishing said authentication ticket, the shelf registration of said authentication ticket is directed to said authentication ticket management tool. Said license server means An authentication system given in either of claims 1-11 characterized by not carrying out use license when the renewal of hysteresis of said authentication ticket is directed to said authentication ticket management tool in response to presentation of said authentication ticket and the notice of refusal is received from said authentication ticket management tool.

[Claim 16] Said license server means two or more preparations and said client means It is what has managed the use count of said authentication ticket, shows this with said authentication ticket, and asks for use license. Said authentication server means Issue hysteresis is memorized while publishing said authentication ticket. Said license server means Memorize updating hysteresis, while updating said authentication ticket, and it refers for the hysteresis of said authentication ticket to said authentication server means which the publisher identifier of said authentication ticket shows in response to presentation of said authentication ticket, or said license server means. The authentication system according to claim 12 characterized by not carrying out use license when the notice of refusal is received from said authentication server means or said license server means.

[Claim 17] It is an authentication system given in either of claims 14-16 which said license server means generates a random number in a use license procedure, and show this, require presentation information, and are characterized by said presentation information in case the use count of said authentication ticket is k being as a result of [of what performed said predetermined irreversible operation to said confidential information $n-k$ times, and said random number] EXCLUSIVE OR operation.

[Claim 18] An authentication server means to publish an authentication ticket, and a license server means to approve use of an authentication ticket, In an authentication

system equipped with a client means to require an authentication ticket of said authentication server means, and to require use license of an authentication ticket of said license server means An input means by which said client means obtains the input of the count of effective of a user-identification child, user authentication information, a server identifier, and an authentication ticket, A ticket maintenance means to obtain and hold an authentication ticket from said authentication server means, and to show said license server means, A processing selection means to acquire the existence information on an authentication ticket and to choose processing from said ticket maintenance means, A hash means to obtain a random number and to perform a hash operation to these connection from said authentication server means while acquiring user authentication information from said input means, A secret storage means to memorize in secrecy the hash value obtained from said hash means, Take out a hash value from said secret storage means, and the count n of effective (n is a positive integer) is obtained from said input means in a user authentication procedure. The multistage hash value which performed and obtained n steps of hash operations for said authentication server means Delivery, In a use license procedure, the count k of use (k is a positive integer below n) is obtained from said license server means. An authentication information storage means by which provided a multistage hash means to send the multistage hash value which performed and obtained the hash operation of a $n-k$ stage to said license server means, and user authentication information was accumulated for said authentication server means, The 2nd multistage hash means which performs $n+1$ step of hash operation to connection by the random-number generation means which generates a random number and is sent to said client means, and the user authentication information acquired from said authentication information storage means and the random number generated with said random-number generation means, An authentication collating means to collate with the multistage hash value which obtained the multistage hash value obtained from said client means with said 2nd multistage hash means, a ticket identifier generation means to generate an effective ticket identifier, and the authentication which clocks time of day and outputs time information -- a time check -- with a means The ticket identifier obtained from said ticket identifier generation means, the multistage hash value obtained from said authentication collating means, the server identifier obtained from said client means and the count of effective, and said authentication -- a time check -- the time stump based on the time information acquired from the means -- An authentication child is added to connection of the publisher identifier which shows an authentication server means to a list. An authentication child verification means to verify the authentication child of the authentication ticket which possessed the authentication child addition means sent to said client means as an authentication ticket, and said license server means obtained from said client means, the license which clocks time of day and outputs time information -- a time check -- a means, the validity of a server identifier and a time

stump, and said license -- a time check -- with a ticket effective judging means to check the effectiveness of a difference with the time information acquired from the means The ticket use management tool which remains with the ticket identifier of an authentication ticket, and the count of use, and manages the count of available, The 3rd multistage hash means which outputs the secondary multistage hash value which performed and obtained k steps of hash operations from said ticket use management tool to the multistage hash value which obtained the count k of use and was obtained from said client means, The authentication system characterized by providing a license collating means to collate the multistage hash value obtained from said ticket use management tool, and the secondary multistage hash value obtained from said 3rd multistage hash means.

[Claim 19] A server common key storage means by which said authentication child addition means memorizes the common key system cryptographic key shared between servers, A data connection means to connect a self-identifier storage means to memorize a self-identifier, and a ticket identifier, a multistage hash value, the count of effective, a time stump, a server identifier and the publisher identifier obtained from said self-identifier storage means, A connection data hash means to perform a hash operation to the connection data obtained from said data connection means, The common key system cryptographer stage which enciphers the hash value obtained from said connection data hash means using the common key system cryptographic key obtained from said server common key storage means, and is made into an authentication child, An authentication child connection means to connect the connection data obtained from said data connection means and the authentication child who got from said common key system cryptographer stage is provided. The 2nd server common key storage means said authentication child verification means remembers the common key system cryptographic key shared between servers to be, An authentication child separation means to divide an authentication ticket into connection data and an authentication child, A data separation means to divide into a ticket identifier, a multistage hash value, the count of effective, a time stump, a server identifier, and a publisher identifier the connection data obtained from said authentication child separation means, The 2nd connection data hash means which performs a hash operation to the connection data obtained from said authentication child separation means, The 2nd common key system cryptographer stage which enciphers the hash value obtained from said 2nd connection data hash means using the common key system cryptographic key obtained from said 2nd server common key storage means, and is made into the authentication child for a comparison, A publisher identifier collating means to confirm that the publisher identifier obtained from said data separation means is an effective server identifier, The authentication system according to claim 18 characterized by providing a comparison means to compare the authentication child for a comparison who got from said 2nd common key system cryptographer stage with the authentication child who got from said

authentication child separation means when the collating result obtained from said publisher identifier collating means showed the owner effect, and to output a result.

[Claim 20] A self-private key storage means by which said authentication child addition means memorizes the public key system code private key of an authentication server in secrecy, A data connection means to connect a self-identifier storage means to memorize a self-identifier, and a ticket identifier, a multistage hash value, the count of effective, a time stump, a server identifier and the publisher identifier obtained from said self-identifier storage means, A connection data hash means to perform a hash operation to the connection data obtained from said data connection means, The public key system cryptographer stage which enciphers the hash value obtained from said connection data hash means using the public key system code private key obtained from said self-private key storage means, and is made into an authentication child, An authentication child separation means by which provide an authentication child connection means to connect the connection data obtained from said data connection means, and the authentication child who got from said public key system cryptographer stage, and said authentication child verification means divides an authentication ticket into connection data and an authentication child, A data separation means to separate and output the connection data obtained from said authentication child separation means to a ticket identifier, a multistage hash value, the count of effective, a time stump, a server identifier, and a publisher identifier, The 2nd connection data hash means which performs a hash operation to the connection data obtained from said authentication child separation means, A server public key are recording means to output the public key system code public key corresponding to the publisher identifier which the public key system code public key of an effective server was accumulated, and was obtained from said data separation means, The public key system decode means which decodes the authentication child who got from said authentication child separation means using the public key system code public key obtained from said server public key are recording means, and is made into the hash value for a comparison, The authentication system according to claim 18 characterized by providing a comparison means to compare the hash value obtained from said connection data hash means with the hash value for a comparison obtained from said public key system decode means, and to output a result.

[Claim 21] Said client means possesses an authentication random-number generation means and the 1st exclusive-OR means. Said random-number generation means for authentication The random number for authentication is generated in a user authentication procedure. Said 1st exclusive-OR means The disturbance hash value which obtained by performing EXCLUSIVE OR operation of the random number for authentication obtained from said random-number generation means for authentication in the user authentication procedure, and the hash value obtained from said hash means for said authentication server means Delivery, Said secret storage

means memorizes in secrecy the random number for authentication obtained from said random-number generation means for authentication. Said multistage hash means Take out the random number for authentication from said secret storage means, and the count k of use is obtained from said license server means in a use license procedure. The multistage hash value which performed and obtained the hash operation of a $n-k$ stage for said license server means Delivery, Said authentication server means possesses the 2nd hash means and the 2nd exclusive-OR means instead of said authentication collating means. Said 2nd hash means A hash operation is performed to connection by the user authentication information acquired from said authentication information storage means, and the random numbers generated with said random-number generation means. Said 2nd exclusive-OR means Perform EXCLUSIVE OR operation of the hash value obtained from said 2nd hash means, and the disturbance hash value obtained from said client means, and the random number for authentication is acquired. Said 2nd multistage hash means performs n steps of hash operations by the random numbers for authentication obtained from said 2nd exclusive-OR means. Said authentication child addition means The ticket identifier obtained from said ticket identifier generation means, the multistage hash value obtained from said 2nd multistage hash means, the server identifier obtained from said client means and the count of effective, and said authentication -- a time check -- the time stamp based on the time information acquired from the means -- An authentication system given in either of claims 18-20 characterized by adding an authentication child to connection of the publisher identifier which shows an authentication server means to a list, and sending to said client means as an authentication ticket.

[Claim 22] Said license server means possesses the 3rd hash means and the 2nd authentication child addition means instead of said 3rd multistage hash means. Said 3rd hash means The secondary multistage hash value which performed and obtained the hash operation to the multistage hash value obtained from said client means is outputted. Said license collating means The multistage hash value obtained from said ticket use management tool and the secondary multistage hash value obtained from said 3rd hash means are collated. Said 2nd authentication child addition means The ticket identifier, the server identifier, and the count of the remaining use which were obtained from said ticket use management tool, the multistage hash value obtained from said client means, and said license -- a time check -- the time stamp based on the time information acquired from the means -- An authentication system given in either of claims 18-21 characterized by adding an authentication child to connection of the publisher identifier which shows a license server means to a list, and sending to said client means as an authentication ticket.

[Claim 23] One or more license server means and the authentication ticket management tool which manages issue of an authentication ticket and a use situation are provided. Said authentication ticket management tool remains with a ticket

identifier and the count of effective based on the authentication ticket shelf registration directions obtained from said authentication server means, and a group with the count of use is managed. Adjustment with the renewal directions of authentication ticket hysteresis obtained from said license server means is checked. In the case of mismatching, delivery and said authentication server means possess a ticket registration directions means for the notice of authentication ticket refusal at said license server means. Said ticket registration directions means Authentication ticket shelf registration directions are generated from the ticket identifier obtained from said ticket identifier generation means, the server identifier obtained from said client means, and the count of effective. To said authentication ticket management tool Delivery, Said client means possesses the ticket maintenance management tool replaced with said ticket maintenance means, and the 1st exclusive-OR means. Said ticket maintenance management tool While obtaining and holding an authentication ticket from said authentication server means, the count of use is managed, and they are shown to said license server means. Said multistage hash means The multistage hash value which took out the hash value from said secret storage means, and performed and obtained n steps of hash operations in the user authentication procedure for said authentication server means Delivery, The count k of use obtained from said ticket maintenance management tool in the use license procedure is obtained. The multistage hash value which performed and obtained the hash operation of a n-k stage for said 1st exclusive-OR means delivery and said 1st exclusive-OR means EXCLUSIVE OR operation of the multistage hash value obtained from said multistage hash means and the random number obtained from said license server means is performed. The disturbance multistage hash value of a result for said license server means Delivery, Said license server means possesses the renewal directions means of a ticket replaced with a ticket use management tool, the 2nd random-number generation means, and the 2nd exclusive-OR means. Said renewal directions means of a ticket The renewal directions of authentication ticket hysteresis are generated from the ticket identifier and server identifier which were obtained from said authentication child verification means when the judgment result obtained from said ticket effective judging means showed the owner effect, and the count of use obtained from said client means. To said authentication ticket management tool Delivery, The count k of use obtained from said client means when the notice of authentication ticket refusal was not returned from said authentication ticket management tool, and the multistage hash value obtained from said authentication child verification means are outputted. Said 2nd random-number generation means generates a random number. For said client means and said 2nd exclusive-OR means delivery and said 2nd exclusive-OR means Perform EXCLUSIVE OR operation of the random number obtained from said 2nd random-number generation means, and the disturbance multistage hash value obtained from said client means, and a multistage hash value is acquired. Said 3rd multistage hash means outputs the secondary

multistage hash value which performed and obtained k steps of hash operations to the multistage hash value obtained from said 2nd exclusive-OR means. Said authentication ticket management tool remains with a ticket identifier and the count of effective based on the authentication ticket shelf registration directions obtained from said authentication server means, and a group with the count of use is managed. An authentication system given in either of claims 18-21 characterized by checking adjustment with the renewal directions of authentication ticket hysteresis obtained from said license server means, and sending the notice of authentication ticket refusal at said license server means in the case of mismatching.

[Claim 24] One or more license server means are provided, and said authentication server means possesses a ticket issue management tool. Said ticket issue management tool The ticket identifier obtained from said ticket identifier generation means, the server identifier obtained from said client means, and the count of effective are managed. Search a ticket identifier based on the ticket use enquiry obtained from said license server means, and the adjustment of the count of use is checked. The ticket maintenance management tool with which delivery and said client means replace the notice of authentication ticket refusal for said ticket maintenance means at said license server means in the case of mismatching, The 1st exclusive-OR means is provided. Said ticket maintenance management tool While obtaining and holding an authentication ticket from said authentication server means, the count of use is managed, and they are shown to said license server means. Said multistage hash means The multistage hash value which took out the hash value from said secret storage means, and performed and obtained n steps of hash operations in the user authentication procedure for said authentication server means Delivery, The count k of use obtained from said ticket maintenance management tool in the use license procedure is obtained. The multistage hash value which performed and obtained the hash operation of a n-k stage for said 1st exclusive-OR means delivery and said 1st exclusive-OR means EXCLUSIVE OR operation of the multistage hash value obtained from said multistage hash means and the random number obtained from said license server means is performed. The disturbance multistage hash value of a result for said license server means Delivery, Said license server means possesses the renewal management tool of a ticket replaced with said ticket use management tool, and the 2nd random-number generation means and the 2nd exclusive-OR means. Said renewal management tool of a ticket Ticket use enquiry is generated from the ticket identifier and server identifier which were obtained from said authentication child verification means when the judgment result obtained from said ticket effective judging means showed the owner effect, and the count of use obtained from said client means. As opposed to said authentication server means or the 2nd license server means which a publisher identifier shows Delivery, When the notice of authentication ticket refusal is not returned from said authentication server means or said 2nd license server means, while outputting the count of use obtained

from said client means, and the multistage hash value obtained from said authentication child verification means When a ticket identifier, a server identifier, and the count of the remaining use are managed and ticket use enquiry is received from said 2nd license server means, the adjustment of the count of use is checked. In the case of mismatching, the notice of authentication ticket refusal at said 2nd license server means delivery and said 2nd random-number generation means A random number is generated. For said client means and said 2nd exclusive-OR means delivery and said 2nd exclusive-OR means EXCLUSIVE OR operation of the random number obtained from said 2nd random-number generation means and the disturbance multistage hash value obtained from said client means is performed, and a multistage hash value is acquired. Said 2nd hash means The secondary multistage hash value which performed and obtained the hash operation to the multistage hash value obtained from said 2nd exclusive-OR means is outputted. Said 2nd authentication child addition means The ticket identifier, the server identifier, and the count of the remaining use which were obtained from said ticket management tool, the multistage hash value obtained from said 2nd exclusive-OR means, and said license -- a time check -- the time stamp based on the time information acquired from the means -- The authentication system according to claim 22 characterized by adding an authentication child to connection of the publisher identifier which shows a license server means to a list, and sending to said client means as an authentication ticket.

[Claim 25] An authentication server means to publish an authentication ticket, and a license server means to approve use of an authentication ticket, In the authentication approach of an authentication system equipped with a client means to require an authentication ticket of said authentication server means, and to require use license of an authentication ticket of said license server means Include n (n is positive integer) time almsgiving ***** information for a predetermined irreversible operation in the confidential information which an authentication server means and a client means share for a client means from an authentication server means. The authentication ticket whose count of effective is n is published. A client means Said authentication ticket is shown in a license server means, it asks for use license, and a demand of the presentation information on a license server means is received. A client means When the use count of said authentication ticket is k (k is a positive integer below n), It is the authentication approach characterized by showing the result of an operation which performed said predetermined irreversible operation to said confidential information $n-k$ times as said presentation information, and for a license server means performing said predetermined irreversible operation to said presentation information k times, and identifying coincidence with the result of an operation and said collating information.

[Claim 26] An authentication server means to publish an authentication ticket, and a license server means to approve use of an authentication ticket, In the authentication approach of an authentication system equipped with a client means to require an

authentication ticket of said authentication server means, and to require use license of an authentication ticket of said license server means Include n (n is positive integer) time almsgiving ***** information for a predetermined irreversible operation in the confidential information which an authentication server means and a client means share for a client means from an authentication server means. The authentication ticket whose count of effective is n is published. A client means Said authentication ticket is shown in a license server means, it asks for use license, and a demand of the presentation information on a license server means is received. A client means When the use count of said authentication ticket is k (k is a positive integer below n), The result of an operation which performed said predetermined irreversible operation to said confidential information $n-k$ times is shown as said presentation information. A license server means The authentication approach characterized by updating the collating information included in said authentication ticket to the result of an operation which performed said predetermined irreversible operation to said confidential information $n-k$ times while performing said predetermined irreversible operation to said presentation information once and identifying coincidence with the result of an operation and said collating information.

[Claim 27] Said authentication server means shows a random number to a client means to require an authentication ticket, and authentication presentation information is required. A client means The result of an operation which performed said predetermined irreversible operation to connection by user authentication information and said random numbers once $[n+]$ is shown as said authentication presentation information. An authentication server means Said predetermined irreversible operation is performed to connection by the user authentication information currently held and said random numbers once $[n+]$. If coincidence with the result of an operation and said authentication presentation information is checked, the result of an operation which performed said predetermined irreversible operation to connection by said user authentication information and said random number once will be made into said confidential information. The authentication approach according to claim 25 or 26 characterized by publishing the authentication ticket which includes n (n is positive integer) time almsgiving ***** collating information for a predetermined irreversible operation in this.

[Claim 28] Said authentication server means shows a random number to a client means to require an authentication ticket, and authentication presentation information is required. A client means The EXCLUSIVE-OR-operation result of what performed said predetermined irreversible operation to connection by user authentication information and said random numbers once or more, and the random number for authentication which the client means generated is shown as said authentication presentation information. An authentication server means counts said random number for authentication backward from said authentication presentation information using the user authentication information currently held and said random number, and

makes said random number for authentication said confidential information. The authentication approach according to claim 25 or 26 characterized by publishing the authentication ticket which includes n (n is positive integer) time almsgiving ***** collating information for a predetermined irreversible operation in this.

[Claim 29] The authentication processing program record medium with which the computer recorded the processing program of the authentication approach performed by the authentication system of a publication by either of claims 1-24, or the authentication approach given in either of claims 25-28 in the format in which read is possible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Client equipment makes cipher processing in client equipment unnecessary, and enables it to process this invention also with equipment with low computation capacity especially about the authentication approach of a single sign-on mold and authentication system which permit access of multiple times with one processing in which the validity of accessing server equipment is judged.

[0002]

[Description of the Prior Art] The server client mold system which consists of the server equipment and client equipment which were connected through the network with development of a digital-communication technique in recent years is general. In such a server client mold system, it is important that it checks that client equipment and its user have the just authority to access server equipment, and unjust access is made not to be performed. Although what is depended on a password input is well known as the authentication approach of checking this access permission, while the method of asking for a password input whenever it accesses is safe, since it is inconvenient, for a user, the authentication approach of the single sign-on mold which raised convenience has come to be used. Generally as the authentication approach of such a single sign-on mold, TTP (Trusted Third-party Protocol) used by the Kerberos authentication system is known, for example.

[0003] Hereafter, it explains, referring to a drawing about the authentication approach of the conventional single sign-on mold. Drawing 23 is the conceptual diagram showing the outline of the authentication approach of the conventional single sign-on mold, and drawing 24 is the protocol sequence diagram showing a protocol. In drawing 23 and drawing 24, they are a client means by which 81 has a user interface, an authentication server means by which 82 performs user authentication, and a license

server means for 83 to judge an access permission and to perform use license.

[0004] In the user authentication procedure of the client means 81 and the authentication server means 82, the authentication server means 82 returns the authentication response Authorize Request802 accompanied by the session key SK with which the client means 81 was enciphered by the authentication server means 82 considering Password PW as a key to delivery and this in authentication demand Authenticate Request801 which became also considering the user-identification child UID inputted through the user interface, and the server identifier SID as authentication presentation information with the authentication ticket Ticket803.

[0005] Furthermore, it sets for the use license procedure of the client means 81 and the license server means 83. The license demand Authorize Request804 which the client means 81 became also considering the user-identification child UID enciphered with the session key SK, and the time stamp TSk as presentation information for the license server means 83 with the authentication ticket Ticket805 Delivery, On the other hand, the license server means 83 verifies the presentation information and the authentication ticket Ticket805 in the authentication demand Authorize Request804, and if it admits being just, it will return the notice Result806 of license.

[0006] It explains in the authentication approach of the conventional single sign-on mold with the above protocol sequences, referring to drawing 25 about the configuration below. Drawing 25 is the functional block diagram showing the configuration of the authentication approach of the conventional single sign-on mold. Also in drawing 25, they are a client means by which 81 has a user interface, an authentication server means by which 82 performs user authentication, and a license server means for 83 to judge an access permission and to perform use license.

[0007] 1st transceiver means 311 by which the client means 81 transmits and receives data, An input means 811 to obtain the input from a user, and a session key decode means 812 to decode the received session key, A ticket maintenance means 314 to hold the received authentication ticket, and a processing selection means 315 to choose processing according to the maintenance condition of an authentication ticket, a secret storage means 316 to memorize the decoded session key in secrecy, and the certification which clocks time of day -- a time check -- it consists of a means 813 and a certification information cryptographer stage 814 which enciphers attested certification information using a session key.

[0008] Moreover, 2nd transceiver means 321 by which the authentication server means 82 transmits and receives data, the authentication which clocks time of day -- a time check -- with a means 322 and an authentication information storage means 323 by which user authentication information, such as a password, was accumulated It consists of a session key generation means 821 to generate a cryptographic key for every user authentication processing, a session key cryptographer stage 822 which enciphers a session key using a password, and a ticket cryptographer stage 823 which enciphers an authentication ticket using a session key.

[0009] Moreover, 3rd transceiver means 331 by which the license server means 83 transmits and receives data, the license which clocks time of day -- a time check -- with a means 332 and a ticket decode means 831 to decode an authentication ticket. A ticket effective judging means 832 to perform the effectiveness judging of an authentication ticket, It consists of license collating means 835 which carry out comparison collating of a certification information decode means 833 to decrypt attested certification information, a certification information effective judging means 834 to perform the effectiveness judging of attested certification information, and the contents of the authentication ticket and the contents of attested certification information.

[0010] It explains in the authentication approach of the conventional single sign-on mold constituted as mentioned above, referring to drawing 26 about the actuation below. First, in the client means 81, the password PW for user authentication beforehand registered into the authentication server means 82 with the user-identification child UID who shows the user itself, and the server identifier SID of the object which obtains use license are inputted into the input means 811 as a user input 800 (ST3101, ST8101). The input means 811 takes out the server identifier 3101, and sends it to the ticket maintenance means 314 while it holds a user input 800 temporarily. The ticket maintenance means 314 searches the authentication ticket data corresponding to the server identifier 3101 (ST3102), and sends the notice 3102 of a retrieval result to the processing selection means 315. The processing selection means 315 sends the notice 8102 of use license procedure starting to said ticket maintenance means 314, the secret storage means 316, and the certification information cryptographer stage 814, when the notice 3102 of a retrieval result shows non-** and delivery and owner ** are shown for the notice 8101 of user authentication processing starting in said input means 811 (ST3103).

[0011] Through the 1st transceiver means 311, as authentication demand Authenticate Request801, delivery (ST8102) and the user-identification child 8104 will be seen off in the certification information cryptographer stage 814, and said input means 811 will see off delivery and a password 8105 for the group 8103 of the user-identification child and server identifier which were taken out from the user input 800 held temporarily to the session key decode means 812 at the authentication server means 82, if the notice 8101 of user authentication starting is given.

[0012] In the authentication server means 82, the user-identification child 8201 from whom authentication demand Authenticate Request801 was received and taken out with the 2nd transceiver means 321 is seen off in the authentication information storage means 323 and the ticket cryptographer stage 823, and the server identifier 8202 is sent to the ticket cryptographer stage 823 (ST8201). The authentication information storage means 323 searches the password corresponding to the user-identification child 8201 (ST8202), and when it is, a password 8203 is sent to the session key cryptographer stage 822, and it sends delivery and the notice 8204 of a

retrieval result to the session key generation means 821 and the session key cryptographer stage 822 (ST8203). When the notice 8204 of a retrieval result shows owner **, the session key generation means 821 newly generates the random session key 8205, and sends it to the session key cryptographer stage 822 and the ticket cryptographer stage 823 (ST8204). When the notice 8204 of a retrieval result shows owner **, the session key cryptographer stage 822 generates the encryption session key 8206 which used the password 8203 and enciphered the session key 8205 (ST8205), and sends this to the client means 81 as authentication response Authenticate Response802 through the 2nd transceiver means 321 (ST8207). authentication -- a time check -- the means 322 has clocked current time and supplies the time stump 3212 based on current time to the ticket cryptographer stage 823. The ticket cryptographer stage 823 generates the authentication ticket data 8207 which held inside and enciphered the user-identification child 8201, the server identifier 8202, the time stump 3212, and the session key 8205 using the server common key corresponding to the server identifier 8202 (ST8202, ST8206), and sends this to the client means 81 as an authentication ticket Ticket803 through the 2nd transceiver means 321 (ST8207).

[0013] In the client means 81, authentication response Authenticate Response802 is sent to the session key decode means 812 as an encryption session key 8106 through the 1st transceiver means 311, and the authentication ticket Ticket803 is sent to said ticket maintenance means 314 as authentication ticket data 8108 through the 1st transceiver means 311 (ST8103). Said ticket maintenance means 314 matches the authentication ticket data 8108 with the server identifier 3101, and holds them (ST3112). The session key decode means 812 decrypts the encryption session key 8106 using a password 8105 (ST8104). Therefore, only when a right password is entered, a right session key can be obtained. The session key 8107 obtained with the session key decode means 812 is sent to the secret storage means 316, and is memorized.

[0014] The secret storage means 316 sends the memorized session key 8109 to the certification information cryptographer stage 814, when the session key 8107 is memorized in secrecy, only predetermined access is permitted and the notice 8102 of use license procedure starting is given (ST8105). certification -- a time check -- the means 813 has clocked current time and supplies the time stump 8110 based on current time to the certification information cryptographer stage 814. If the notice 8102 of use license procedure starting is given, the certification information cryptographer stage 814 will generate the attested certification information 8111 which enciphered the user-identification child 8104 and the time stump 8110 using the session key 8109 (ST8106), and will send this to the license server means 83 as license demand Authorize Request804 through the 1st transceiver means 311 (ST8107). Said ticket maintenance means 314 will send the held authentication ticket data 8112 corresponding to the server identifier 3101 to the license server means 83

as an authentication ticket Ticket805 through the 1st transceiver means 311, if the notice 8102 of use license procedure starting is given (ST8107).

[0015] In the license server means 83, the license demand Authorize Request804 is sent to the certification information decode means 833 as attested certification information 8308 through the 3rd transceiver means 331, and the authentication ticket Ticket805 is sent to the ticket decode means 831 as authentication ticket data 8301 through the 3rd transceiver means 331 (ST8301). Decrypt the ticket decode means 831 using the self-server common key which held the authentication ticket data 8301 inside, the user-identification child 8302 and the server identifier 8303 which were obtained, and a time stamp 8304 are sent to the ticket effective judging means 832, and delivery and the session key 8305 are sent to the certification information decode means 833 (ST8302). license -- a time check -- the means 332 has clocked current time and supplies the current time information 8306 to the ticket effective judging means 832 and the certification information effective judging means 834. The ticket effective judging means 832 confirms that the difference of a time stamp 8304 and the current time information 8306 is within the limits of a predetermined expiration date, when all are truth, makes the user-identification child 8302 the ticket user-identification child 8307, and sees him off in the license collating means 835, while it performs the coincidence judging with the server identifier 8303 and the self-server identifier held inside (ST3306, ST3307). The certification information decode means 833 decrypts the attested certification information 8308 using the session key 8305, and the user-identification child 8309 and time stamp 8310 which were obtained are sent to the certification information effective judging means 834 (ST8303). Since attested certification information is enciphered using the session key with the client means, only when a right session key is used with a client means, a right user-identification child and a time stamp are obtained here. The certification information effective judging means 834 confirms that the difference of a time stamp 8310 and the current time information 8306 is within the limits of predetermined time difference, when it is truth, makes the user-identification child 8309 the certification user-identification child 8311, and sees him off in the license collating means 835 (ST8304, ST8305). The license collating means 835 performs the coincidence judging with the ticket user-identification child 8307 and the certification user-identification child 8311 (ST8306), and if it is truth, the client means 81 will receive the notice 8312 of license in delivery (ST8307, ST3317) and the client means 81 through the 3rd transceiver means 331 as notice Result806 of license (ST3118). When a coincidence judging becomes truth at this time, the user-identification child and the time stamp are obtained correctly, this shows that the right session key was used with the client means, and since this means that the right password was entered, a user authentication result and its use license result will correspond.

[0016]

[Problem(s) to be Solved by the Invention] However, since cipher processing which

needs great computational complexity with the above-mentioned conventional configuration was used abundantly and it was necessary to perform cipher processing at every use license processing by the client side especially, when client sides were a personal digital assistant and low equipment of computation capacity like a smart phone, it had the technical problem that it was difficult to perform use license processing by the practical processing time.

[0017] Moreover, even if the code of the authentication ticket which did not restrict the use count of one authentication ticket, but was intercepted by the third person with the above-mentioned conventional configuration since it was only having prepared the expiration date should have been decoded and unjust access was performed, it also had the technical problem that possibility of finishing without being discovered was high.

[0018] This invention does not solve such a conventional technical problem, does not need cipher processing in a client side, but even if it is low equipment of computation capacity, it can perform use license processing by the practical processing time, and it aims at offering the authentication approach of a single sign-on mold and authentication system which can manage the use count of an authentication ticket easily.

[0019]

[Means for Solving the Problem] A client means for this invention to hold the authentication ticket whose count of effective is n (n is a positive integer) to the 1st, and for this to be shown, and to ask for use license in order to solve this technical problem, In response, presentation information is required and it prepares with the license server means which collates with said authentication ticket and carries out use license. Said authentication ticket An authentication child is given including a ticket identifier, collating information, the count of effective, the time of the date of issue, and a server identifier. Said collating information A predetermined irreversible operation is performed to the confidential information which the publisher and said client means of said authentication ticket share n times. Said presentation information in case the use count of said authentication ticket is k (k is a positive integer below n) is characterized by performing said predetermined irreversible operation to said confidential information $n-k$ times.

[0020] The authentication approach of a single sign-on mold and authentication system which cannot need cipher processing in a client side, but can manage the use count of an authentication ticket easily by this, and can eliminate duplex use are obtained.

[0021] It is characterized by for said authentication server means generating a random number in a user authentication procedure, and showing this in the 2nd, requiring authentication presentation information of a client means, for said confidential information performing said predetermined irreversible operation to connection by said user authentication information and said random number once or

more, and said authentication presentation information performing said predetermined irreversible operation to said confidential information n times.

[0022] The authentication approach of a single sign-on mold and authentication system which can communalize data processing of authentication presentation information and data processing of presentation information by this in not needing cipher processing in a client side in a user authentication procedure in addition to the above-mentioned effectiveness are obtained.

[0023] It is what said authentication server means generates a random number in a user authentication procedure to the 3rd, shows this to it, and requires authentication presentation information of a client means. Said authentication presentation information It is as a result of [of what performed said predetermined irreversible operation to connection by said user authentication information and said random number once or more, and the random number for authentication which the client means generated] EXCLUSIVE OR operation, and said confidential information is characterized by being said random number for authentication counted backward from said authentication presentation information.

[0024] Since the collating information included in an authentication ticket becomes unrelated to user authentication information by this in addition to the above-mentioned effectiveness, the authentication approach of a safer single sign-on mold and authentication system which even possibility that user authentication information will be guessed does not have are obtained from an authentication ticket.

[0025] It is characterized by on the other hand said predetermined irreversible operation being a tropism hash operation the 4th.

[0026] Thereby, in addition to the above-mentioned effectiveness, even if a client side is low equipment of computation capacity, the authentication approach of a single sign-on mold and authentication system which can perform use license processing by the practical processing time are obtained.

[0027] It is characterized by for said authentication ticket updating the collating information on said authentication ticket, the count of effective, the time of the date of issue, a publisher identifier, and an authentication child to the 5th, including a publisher identifier, while said license server means carries out use license, and for said collating information being what performed said predetermined irreversible operation $n-k$ times at said confidential information, being updated, and updating said count of effective by $n-k$.

[0028] Since it is updated in addition to the above-mentioned effectiveness by this whenever it uses an authentication ticket, especially a time stamp is updated and the expiration date in an effective judging can be set up shorter, possibility of the unauthorized use by the third person can be made smaller, and the authentication approach of the single sign-on mold which can shorten the response time of use license further, and an authentication system are obtained.

[0029] To the 6th, said client means has managed the use count of said

authentication ticket. It is what shows this and asks for use license with said authentication ticket. It has the authentication ticket management tool which manages the use count of two or more preparations and said authentication ticket for said license server means. Said authentication server means While publishing said authentication ticket, the shelf registration of said authentication ticket is directed to said authentication ticket management tool. Said license server means When the renewal of hysteresis of said authentication ticket is directed to said authentication ticket management tool in response to presentation of said authentication ticket and the notice of refusal is received from said authentication ticket management tool, it is characterized by not carrying out use license.

[0030] Since this becomes possible to use an authentication ticket in common to two or more license servers in the system by which an authentication ticket is not updated in addition to the above-mentioned effectiveness, the authentication approach of a single sign-on mold and an authentication system with more high convenience are obtained.

[0031] To the 7th, said client means has managed the use count of said authentication ticket. It is what shows this and asks for use license with said authentication ticket. Said license server means two or more preparations and said authentication server means Issue hysteresis is memorized while publishing said authentication ticket. Said license server means Memorize updating hysteresis, while updating said authentication ticket, and it refers for the hysteresis of said authentication ticket to said authentication server means which the publisher identifier of said authentication ticket shows in response to presentation of said authentication ticket, or said license server means. When the notice of refusal is received from said authentication server means or said license server means, it is characterized by not carrying out use license.

[0032] Thereby, since the distributed management of the use of an authentication ticket can be carried out in the system by which an authentication ticket is updated in addition to the above-mentioned effectiveness, the authentication approach of a single sign-on mold and authentication system which can lessen one management resource more are obtained.

[0033]

[Embodiment of the Invention] Hereafter, it explains, referring to a drawing about the gestalt of operation of this invention.

[0034] (Gestalt of the 1st operation) The authentication system of the 1st operation gestalt consists of the client means 1 with a user interface, an authentication server means 2 to perform user authentication, and a license server means 3 to judge the access permission of the client means 1 and to perform use license, as shown in drawing 1 . A general purpose computer, a Personal Digital Assistant, a smart phone, etc. can be used for the client means 1, and a general purpose computer, exclusive authentication server equipment, etc. can be used for the authentication server

means 2, and a general purpose computer, exclusive license server equipment, exclusive information offer equipment, etc. can be used for the license server means 3.

[0035] A cable or a radio network connects between the client means 1 and the license server means 3. Although it does not necessarily connect between the client means 1 and the authentication server means 2 in a communication network, it is necessary to share confidential information 4. As this confidential information 4, a password, a common key system cryptographic key, or the calculated value computed from them is used, for example.

[0036] The client means 1 holds the authentication ticket 5 used in a use license procedure. The authentication server means 2 publishes this to the client means 1, and the authentication server means 2 makes collating information the result of having performed the irreversible operation f to confidential information 4 n times (n being the count of effective of an authentication ticket), adds an authentication child to this, and generates the authentication ticket 5. An authentication child is added for the purpose of alteration prevention of an authentication ticket and a publisher's certification, and can use a message authorization code, a digital signature, etc.

[0037] In the use license procedure of the client means 1 and the license server means 3, the result to which the client means 1 performed the irreversible operation f to confidential information 4 the $n-k$ time (k is a use count in the use license procedure of an authentication ticket) is used as presentation information 6. As long as the irreversible operation f has sufficiently safe irreversibility, the die length of a result, and random nature, since the third person who does not know confidential information 4 cannot calculate this presentation information 6, it is shown that it is the valid user which gets to know confidential information 4 using this presentation information 6. Moreover, since many counts of the irreversible operation f in presentation information are performed so that it went back in the past and the following presentation information is also incalculable from this presentation information 6, there is also no need for encryption.

[0038] With the authentication ticket 7 holding this presentation information 6, a client means 1 will return the notice 8 of license, if the check of it being in agreement at the collating information which the authentication ticket 7 includes [the result of having carried out the irreversible operation f to the presentation information 6 k times with verification of the authentication child whom the authentication ticket 7 contains, as for the license server means 3] to delivery and this at the license server means 3 is carried out and it accepts that it is just.

[0039] By this approach, the client means 1 can obtain use license to n times using the authentication ticket 7, without revealing confidential information 4 to a third person including the license server means 3.

[0040] Thus, the authentication system of the gestalt of this operation possesses a client means to hold the authentication ticket whose count of effective is n (n is a

positive integer), and for this to be shown, and to ask for use license, and the license server means which requires presentation information in response, collates with said authentication ticket, and carries out use license.

[0041] At the time of a ticket identifier, the count of effective, and the date of issue, information other than collating information, such as a server identifier, can be included, and an authentication child is given to said authentication ticket at this. Collating information is the information which performed the predetermined irreversible operation to the confidential information which the publisher and client means of an authentication ticket share n times. Moreover, said presentation information is the information which performed the predetermined irreversible operation to said confidential information $n-k$ times, when the use count of an authentication ticket is k (k is a positive integer below n).

[0042] The authentication approach of a single sign-on mold and authentication system which cannot need cipher processing in a client side, but can manage the use count of an authentication ticket easily, and can eliminate duplex use by such configuration are obtained.

[0043] (Gestalt of the 2nd operation) In the authentication system of the 2nd operation gestalt, a client means shows authentication presentation information to the authentication server means 22, and requires an authentication ticket.

[0044] It consists of a license server means 3 for this authentication system to judge the access permission of the client means 11 which has a user interface as shown in drawing 2, an authentication server means 12 to perform user authentication, and the client means 11, and to perform use license, and the cable or the radio network connects between the client means 11, the authentication server means 12, and the license server means 3. This license server means 3 is the same as that of the 1st operation gestalt (drawing 1), and the same as that of the 1st operation gestalt (drawing 1) also about the authentication ticket returned to the client means 11 from the authentication server means 12, the presentation information which the client means 11 transmits to the license server means 3 and a license ticket, and the notice 8 of license further returned to the client means 11 from the license server means 3.

[0045] The client means 11 and the authentication server means 12 of this authentication system share the result of having performed the irreversible operation f to connection by the password PW entered through the user interface, and the random numbers R obtained from the authentication server means 12 once, as confidential information 14. As long as the irreversible operation f has sufficiently safe irreversibility, the die length of a result, and random nature, the third person who does not know Password PW cannot calculate this confidential information 14.

[0046] In the user authentication procedure of the client means 11 and the authentication server means 12, the authentication server means 12 generates a random number, this is shown, and authentication presentation information is required

of the client means 11. The client means 11 computes confidential information 14 by performing the irreversible operation f to connection by Password PW and the random numbers R obtained from the authentication server means 12 once, and sends it to the authentication server means 12 by making into the authentication presentation information 13 the result of having performed the irreversible operation f to this confidential information 14 further n times ($n+1$ total and n being the count of effective of an authentication ticket).

[0047] On the other hand, a check of that the confidential information 14 of the authentication server means 12 corresponds from the authentication presentation information 13 returns the authentication ticket 5 which added the authentication child to this by making into collating information the result of having performed the irreversible operation f to confidential information 14 n times. The client means 11 is held in order to use this in a use license procedure. An authentication child is added for the purpose of alteration prevention of an authentication ticket and a publisher's certification, and can use a message authorization code, a digital signature, etc.

[0048] Moreover, in the use license procedure of the client means 11 and the license server means 3, the result to which the client means 11 performed the irreversible operation f to confidential information 14 the $n-k$ time (k is a use count in the use license procedure of an authentication ticket) is used as presentation information 6. As long as the irreversible operation f has sufficiently safe irreversibility, the die length of a result, and random nature, since the third person who does not know confidential information 14 cannot calculate this presentation information 6, it is shown that it is the valid user which gets to know confidential information 14 using this presentation information 6. Moreover, since many counts of the irreversible operation f in presentation information are performed so that it went back in the past and the following presentation information is also incalculable from this presentation information 6, there is also no need for encryption.

[0049] The check of it being in agreement with the license server means 3 with the authentication ticket 7 holding this presentation information 6 at the collating information which the authentication ticket 7 includes [the result of having carried out the irreversible operation f to the presentation information 6 k times with verification of the authentication child whom the authentication ticket 7 contains, as for the license server means 3] to delivery and this carries out, and a client means 11 will return the notice 8 of license, if it accepts that it is just.

[0050] By this approach, the client means 11 can obtain use license to n times using the authentication ticket 7, without revealing confidential information 14 and Password PW to a third person including the license server means 3.

[0051] Thus, in the authentication system of the gestalt of this operation, an authentication server means generates a random number in a user authentication procedure, shows this, and requires authentication presentation information of a client means. What performed the predetermined irreversible operation to connection by

user authentication information and random numbers once or more as confidential information at this time is used, and what performed the predetermined irreversible operation to this confidential information n times as authentication presentation information is shown.

[0052] By such configuration, the authentication approach of a single sign-on mold and authentication system which in addition to the effectiveness of the 1st operation gestalt cipher processing in a client side is unnecessary, and can communalize data processing of authentication presentation information and data processing of presentation information also in a user authentication procedure are obtained.

[0053] (Gestalt of the 3rd operation) As shown in drawing 3, the random number for authentication generated by the client means 21 is shared between the client means 21 and the authentication server means 22 as confidential information 24 by the authentication system of the 3rd operation gestalt.

[0054] In this system, in a user authentication procedure, the authentication server means 22 generates a random number, this is shown, and authentication presentation information is required of the client means 21. The client means 21 is sent to the authentication server means 22 by making into the authentication presentation information 23 the exclusive-OR result of the result of having performed the irreversible operation f to connection by Password PW and the random numbers R obtained from the authentication server means 22 once, and the confidential information 24 which the client means 21 generated in secrecy. In drawing 3, the notation "@" shows the exclusive-OR (EXOR) operation.

[0055] On the other hand, the authentication server means 22 is counted backward from the authentication presentation information 23, Password PW, and a random number R, and asks for confidential information 25. And the irreversible operation f is performed to this confidential information 25 n times, that result of an operation is made into collating information, and the authentication ticket 5 which added the authentication child to this is returned to the client means 21. The client means 21 is held in order to use this in a use license procedure.

[0056] In addition, if the authentication presentation information 23 was suitably made from the third person with an inaccurate user, even if the authentication ticket 5 can come to hand with the client means 21, the client means 21 does not understand the confidential information 25 which the server counted backward using Password PW and the random number R from the authentication presentation information 23. Therefore, the unjust access can be eliminated in a consecutive use license procedure.

[0057] In the use license procedure of the client means 21 and the license server means 3, the result to which the client means 21 performed the irreversible operation f to confidential information 24 the n-k time (k is a use count in the use license procedure of an authentication ticket) is used as presentation information 6. As long as the irreversible operation f has sufficiently safe irreversibility, the die length of a

result, and random nature, since the third person who does not know confidential information 24 cannot calculate this presentation information 6, it is shown that it is the valid user which gets to know confidential information 24 using this presentation information 6. Moreover, since many counts of the irreversible operation f in presentation information are performed so that it went back in the past and the following presentation information is also incalculable from this presentation information 6, there is also no need for encryption.

[0058] The check of it being in agreement with the license server means 3 with the authentication ticket 7 holding this presentation information 6 at the collating information which the authentication ticket 7 includes [the result of having carried out the irreversible operation f to the presentation information 6 k times with verification of the authentication child whom the authentication ticket 7 contains, as for the license server means 3] to delivery and this carries out, and a client means 21 will return the notice 8 of license, if it accepts that it is just.

[0059] By this approach, the client means 21 can obtain use license to n times using the authentication ticket 7, without revealing confidential information 24 and Password PW to a third person including the license server means 3.

[0060] Thus, in the authentication system of the gestalt of this operation, an authentication server means generates a random number in a user authentication procedure, shows this, and requires authentication presentation information of a client means. Authentication presentation information is as a result of [of what performed the predetermined irreversible operation to connection by user authentication information and said random numbers once or more, and the random number for authentication (confidential information) which the client means generated] EXCLUSIVE OR operation, and this confidential information is counted backward from authentication presentation information by the authentication server means.

[0061] By such configuration, the collating information which an authentication ticket includes becomes unrelated to user authentication information. Therefore, the safe authentication approach of a single sign-on mold and a safe authentication system are obtained rather than even possibility that user authentication information will be guessed from an authentication ticket cannot be found.

[0062] (Gestalt of the 4th operation) The 4th operation gestalt explains the block configuration of each means to perform the concrete communication procedure and concrete it in the authentication system of the 2nd operation gestalt.

[0063] Drawing 4 is the protocol sequence diagram showing the protocol in this system. In drawing 4, a client means by which 31 has a user interface, an authentication server means by which 32 performs user authentication, and a license server means for 33 to judge an access permission and to perform use license are shown, and the notation "S (K|-)" shows the authentication child attachment function which used Key K.

[0064] In the user authentication procedure of the client means 31 and the

authentication server means 32, the client means 31 first sends authentication demand Authenticate Request301 accompanied by the user-identification child UID and the server identifier SID which were inputted through the user interface to the authentication server means 32. At this time, authentication demand Authenticate Request301 is good also as a thing accompanied by the count n of effective of an authentication ticket. When that is not right, an authentication server shall just appoint the count n of effective fixed.

[0065] On the other hand, the authentication server means 32 returns the authentication challenge Challenge302 accompanied by the random number $R0$ generated so that it might differ each time. The client means 31 which received this returns the authentication challenge response Response303 accompanied by the result of having performed $n+1$ step of hash operation H to connection by Password PW and the random number $R0$ which were inputted through the user interface. On the other hand, if the authentication server means 32 carries out comparison verification of the $n+1$ -step hash result of an operation in the challenge response Response303, and the $n+1$ -step hash result of an operation performed itself and is in agreement, it will admit being just. The authentication ticket Ticket304 with which the authentication child was added with the publisher identifier IID which shows ticket identifier TID and the $n+1$ -step hash result of an operation, time stamp TS 0 and server identifier SID, and authentication server 32 self is returned. [which were newly generated] The client means 31 is held in order to use this in a use license procedure.

[0066] Moreover, in the use license procedure of the client means 31 and the license server means 33, the client means 31 sends the license demand Authorize Request and the authentication ticket Ticket305 to the license server means 33. At this time, the license demand Authorize Request is good also as a thing accompanied by the user-identification child UID. On the other hand, the license server means 33 returns the license challenge Challenge306 accompanied by the value k based on the use count of this authentication ticket. The client means 31 which received this returns the license challenge response Response307 accompanied by the result of having performed the hash operation H of +one step of $n-k$ to connection by Password PW and random numbers $R0$.

[0067] As long as it, on the other hand, has tropism, the die length of a result, and random nature, since the third person this hash operation H of whose is insurance enough and who does not know Password PW and a random number $R0$ cannot calculate this hash result of an operation, it is shown that it is the valid user which gets to know Password PW by this hash result of an operation. Moreover, since many number of stageses of the hash operation H are performed so that it went back in the past and the following hash result of an operation is also incalculable from this hash result of an operation, there is also no need for encryption. As such a hash operation [like] H , algorithms, such as MD5 and SHA, can be used, for example.

[0068] On the other hand, the license server means 32 carries out comparison verification of the result of having performed k more steps of hash operations to the $+1$ step of $n-k$ hash result of an operation in the license challenge response Response307, and the $n+1$ -step hash result of an operation in the authentication ticket Ticket, if in agreement, will admit being just and will return the notice Result308 of license. At this time, the notice 308 of license is good also as a thing accompanying coincidence for the information Info to which access was permitted by use license.

[0069] By the above protocol sequences, the client means 31 can obtain use license to n times using the authentication ticket 304, without revealing Password PW to a third person including the license server means 33.

[0070] It explains referring to the functional block diagram of drawing 5 about the configuration with such a protocol sequence of an authentication system.

[0071] In drawing 5, they are a client means by which 31 has a user interface, an authentication server means by which 32 performs user authentication, and a license server means for 33 to judge an access permission and to perform use license.

[0072] 1st transceiver means 311 by which the client means 31 transmits and receives data, An input means 312 to obtain the input from a user, and a hash means 313 to connect two inputs and to perform the hash operation H, A ticket maintenance means 314 to hold the received authentication ticket, and a processing selection means 315 to choose processing according to the maintenance condition of an authentication ticket, It has a multistage hash means 317 to perform the hash operation of a secret storage means 316 to memorize the hash result of an operation in secrecy, and the given number of stages or the number of stages of the difference of two given numeric values.

[0073] The 1st transceiver means 311 is good also as a configuration which consists of infrared interface devices, such as wireless interface devices, such as telephone interface devices, such as ISDN interface devices, such as LAN interface devices, such as a LAN card, and a terminal adopter, and a modem, a pocket data communication card, and a PIAFS card, and an IrDA module, etc., corresponding to the class of communication network, and uses these some properly according to a communications partner. The input means 312 consists of combination of pointing devices and selection carbon buttons, such as alphabetic character input devices, such as a keyboard and a ten key, a mouse, a trackball, and a pen tablet, or a dial and a display screen, or a touch panel. The hash means 313 is constituted combining a logical circuit and the arithmetic circuit incorporating the algorithm of the hash operation H. As for the ticket maintenance means 314, a memory circuit is used. A logical circuit can be used for the processing selection means 315. The secret storage means 316 is constituted by the memory device with Tampa-proof nature like an IC card. The multistage hash means 317 adds the arithmetic circuit which searches for the difference of the counter which counts the connection which feeds back an output to the arithmetic circuit incorporating the algorithm of for example,

the hash operation H, and a number of stages, or a numeric value, and is constituted. In addition, each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or the computer program may be recorded on a program documentation medium in the format in which read is possible, and the configuration combined with the program documentation medium reader may realize.

[0074] Moreover, 2nd transceiver means 321 by which the authentication server means 32 transmits and receives data, the authentication which clocks current time -- a time check -- with a means 322 and an authentication information storage means 323 to accumulate user authentication information, such as a password it gives with a random-number generation means 324 to generate a random number for every user authentication processing -- having -- reliance -- 1 -- with the 2nd multistage hash means 325 which performs the hash operation H of many number of stageses It has the authentication collating means 326 which carries out comparison collating of the two multistage hash values, a ticket identifier generation means 327 to generate a unique ticket identifier for every authentication ticket issue, and an authentication child addition means 328 to generate and add the authentication child to an authentication ticket.

[0075] The 2nd transceiver means 321 consists of infrared interface devices, such as wireless interface devices, such as telephone interface devices, such as ISDN interface devices, such as LAN interface devices, such as a LAN card, and a terminal adopter, and a modem, a pocket data communication card, and a PIAFS card, and an IrDA module, etc., corresponding to the class of communication network.

authentication -- a time check -- as for a means 322, a timer counter is used. If the authentication information storage means 323 is the memory device which consisted of mass memory devices and had the Tampa-proof nature, in addition, it is good. The random-number generation means 324 consists of an arithmetic circuit incorporating for example, a random-number generation algorithm, or an inverter which data-izes an electromagnetic noise. The 2nd multistage hash means 325 adds the counter which counts the connection which feeds back an output to the arithmetic circuit incorporating the algorithm of for example, the hash operation H, and a number of stages, and is constituted. The authentication collating means 326 consists of comparator circuits. The ticket identifier generation means 327 consists of counter circuits which had sufficient bit length, for example. The authentication child addition means 328 consists of the arithmetic circuits and memory circuits incorporating an authentication child generation algorithm. In addition, each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or the computer program may be recorded on a program documentation medium in the format in which read is possible, and the configuration combined with the program documentation medium reader may realize.

[0076] Moreover, 3rd transceiver means 331 by which the license server means 33

transmits and receives data, the license which clocks current time -- a time check -- with a means 332 and an authentication child verification means 333 to verify the authentication child added to the authentication ticket A ticket effective judging means 334 to perform the effectiveness judging of an authentication ticket, It has the ticket use management tool 335 which remains with the ticket identifier of an authentication ticket, and the count of effective, and manages the count of available, the 3rd multistage hash means 336 which performs the hash operation H of the given number of stages, and the license collating means 337 which carries out comparison collating of the two multistage hash values.

[0077] The 3rd transceiver means 331 consists of infrared interface devices, such as wireless interface devices, such as telephone interface devices, such as ISDN interface devices, such as LAN interface devices, such as a LAN card, and a terminal adopter, and a modem, a pocket data communication card, and a PIAFS card, and an IrDA module, etc., corresponding to the class of communication network. license -- a time check -- as for a means 332, a timer counter is used. The authentication child verification means 333 consists of the arithmetic circuits and memory circuits incorporating an authentication child verification algorithm. The ticket effective judging means 334 is constituted by the combination of a comparator circuit. The ticket use management tool 335 is constituted by the combination of the arithmetic circuit which calculates the count of use, and a mass memory device. The 3rd multistage hash means 336 is a change thing, and the preset value of a counter consists of the same arithmetic circuits as the 2nd multistage hash means 325. The license collating means 337 consists of comparator circuits. In addition, each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or the computer program may be recorded on a program documentation medium in the format in which read is possible, and the configuration combined with the program documentation medium reader may realize.

[0078] It explains in the authentication approach and authentication system which were constituted as mentioned above, referring to drawing 6 about the actuation below. Here, the case where authentication demand Authenticate Request301 is accompanied by the count n of authentication ticket effective is explained.

[0079] First, in the client means 31, the password PW for user authentication beforehand registered into the authentication server means 32 with the user-identification child UID who shows the user itself, the server identifier SID of the object which obtains use license, and the count n of effective of an authentication ticket are inputted into the input means 312 as a user input 300 (ST3101, ST3104). The input means 312 takes out the server identifier 3101, and sends it to the ticket maintenance means 314 while it holds a user input 300 temporarily. The ticket maintenance means 314 searches the authentication ticket data corresponding to the server identifier 3101 (ST3102), and sends the notice 3102 of a retrieval result to the processing selection means 315. The processing selection means 315 sends the

notice 3104 of (ST3103) use license procedure starting to said ticket maintenance means 314, the secret storage means 316, and the multistage hash means 317, when the notice 3102 of a retrieval result shows non-**, and delivery and owner ** are shown for the notice 3103 of user authentication processing starting in said input means 312 and the multistage hash means 317.

[0080] Through the 1st transceiver means 311, as authentication demand Authenticate Request301, delivery (ST3105) and the count 3106 of effective will be sent to the multistage hash means 317, and said input means 312 will send delivery and a password 3107 for the group 3105 of the user-identification child and server identifier which were taken out from the user input 300 held temporarily, and the count of effective to the hash means 313 at the authentication server means 32, if the notice 3103 of user authentication starting is given.

[0081] In the authentication server means 32, the user-identification child 3201 from whom authentication demand Authenticate Request301 was received and taken out with the 2nd transceiver means 321 is seen off in the authentication information storage means 323, the count 3202 of effective is sent to the 2nd multistage hash means 325 and the authentication child addition means 328, and the server identifier 3203 is sent to the authentication child addition means 328 (ST3201). The authentication information storage means 323 searches the password corresponding to the user-identification child 3201 (ST3202), and when it is, (ST3203) and a password 3204 are sent to the 2nd multistage hash means 325, and it sends delivery and the notice 3205 of a retrieval result to the random-number generation means 324 and the 2nd multistage hash means 325.

[0082] The random-number generation means 324 is sent to the client means 31 as authentication challenge Challenge302 through the 2nd transceiver means 321 while it newly generates the challenge random number 3206 for data disturbance at random, and sends it to the 2nd multistage hash means 325, when the notice 3205 of a retrieval result shows owner ** (ST3204). the case where, as for the 2nd multistage hash means 325, the notice 3205 of a retrieval result shows owner ** -- connection by the password 3204 and the challenge random numbers 3206 -- receiving -- the count 3202 of effective -- 1 -- the hash operation H of many number of stageses is performed, and the multistage hash value 3207 of a result is sent to the authentication collating means 326 (ST3205).

[0083] On the other hand, in the client means 31, it is received by the 1st transceiver means 311, the challenge random number 3108 is taken out, and the authentication challenge Challenge302 is sent to the hash means 313 (ST3106). The hash means 313 performs the hash operation H to connection by the password 3107 and the challenge random numbers 3108 (ST3107), and sends the hash value 3109 of a result to the secret storage means 316 and the multistage hash means 317. The secret storage means 316 memorizes a hash value 3109 in secrecy, and permits only predetermined access, i.e., the renewal of an addition in a user authentication procedure and the

reference in a use license procedure, (ST3108). When the notice 3103 of user authentication procedure starting is given, the multistage hash means 317 performs the hash operation H of the number of stages equivalent to the count 3106 of effective to a hash value 3109 (ST3109), and sends the multistage hash value 3114 of a result to the authentication server means 32 as authentication challenge response Response303 through the 1st transceiver means 311 (ST3110).

[0084] On the other hand, in the authentication server means 32, it is received by the 2nd transceiver means 321, the multistage hash value 3208 is taken out, and the authentication challenge response Response303 is sent to the authentication collating means 326 (ST3206). The authentication collating means 326 is sent to the authentication child addition means 328 as it is by making the multistage hash value 3208 into the multistage hash value 3210 while it performs the coincidence judging with the multistage hash value 3207 and the multistage hash value 3208 (ST3207) and sends the collating result 3209 to the ticket identifier generation means 327. When the collating result 327 shows coincidence, the ticket identifier generation means 327 generates the effective ticket identifier 3212, and sends it to the authentication child addition means 328 (ST3208).

[0085] authentication -- a time check -- the means 322 has clocked current time and supplies the time stamp 3211 based on current time to the authentication child addition means 328. The authentication child addition means 328 connects the publisher identifier which shows ticket identifier 3212, multistage hash value 3210, count [of effective] 3202, time stamp 3211, server identifier 3203, and authentication server 32 self, generates and adds an authentication child to this, uses him as the authentication ticket data 3213 (ST3209), and is sent to the client means 31 as an authentication ticket Ticket304 through the 2nd transceiver means 321 (ST3210).

[0086] On the other hand, in the client means 31, it is received by the 1st transceiver means 311, the authentication ticket data 3110 are taken out, and the authentication ticket Ticket304 is sent to said ticket maintenance means 314 (ST3111). the case where matched said ticket maintenance means 314 with the server identifier 3101, it held the authentication ticket data 3110 (ST3112), and the notice 3104 of use license procedure starting is given -- the authentication ticket data 3111 -- the 1st transceiver means 311 -- minding -- as the authentication ticket Ticket305 -- the license demand Authorize Request -- the license server means 33 -- sending (ST3113) -- the count 3112 of effective is taken out from authentication ticket data, and it sends to the multistage hash means 317.

[0087] On the other hand, in the license server means 33, it is received by the 3rd transceiver means 331, the authentication ticket data 3301 are taken out, and the license demand Authorize Request accompanied by the authentication ticket Ticket305 is sent to the authentication child verification means 333 (ST3301). The authentication child verification means 333 takes out a time stamp 3302 and the

server identifier 3303 from data division, takes out the ticket identifier 3305, the multistage hash value 3306, the count 3307 of effective, and the publisher identifier 3308 for the ticket effective judging means 334, and sends them to it at the ticket use management tool 335, respectively while it verifies adjustment with data divisions other than the authentication child of the authentication ticket data 3301, and an authentication child and sends the verification result 3304 to the ticket effective judging means 334 (ST3304).

[0088] license -- a time check -- the means 332 has clocked current time and supplies the time stamp 3309 based on current time to the ticket effective judging means 334. The ticket effective judging means 334 confirms that the difference of a time stamp 3302 and the time stamp 3309 based on current time is within the limits of a predetermined expiration date (ST3306, ST3307), and when all are truth, it sends the ticket effective notice 3310 to the ticket use management tool 335, while it performs the coincidence judging with (ST3305), the server identifier 3303, and the self-server identifier held inside (ST3302, ST3303), when the verification result 3304 shows those without an error. If this expiration date is set up short, although security will improve, if user convenience falls and is set up for a long time, user convenience will improve, but since security falls, it should take into consideration and define these balance. For example, what is necessary is just to carry out in 12 hours in 8 hours which can cover the office hours on the 1st, if it applies to the business-use system by which severe security is not demanded. however -- the shortest -- the communication link time amount between a client - a server -- and -- each -- a time check -- it can be necessary to cover the time-of-day error between means

[0089] When the ticket use management tool 335 has managed the ticket list at this time and the ticket effective notice 3310 is given, it investigates whether the ticket identifier 3305 is used, under a ticket list is searched, and it is already registered (ST3308). If there is nothing corresponding, the group of the count 3307 of effective as a value which remains with the ticket identifier 3305 and the count 3307 of effective, and shows the count of available will be added to a ticket list, and will be memorized (ST3309, ST3310). At this time, you may memorize in accordance with the multistage hash value 3306 and the publisher identifier 3308. It receives constructing. the case where there is this added group or a thing which corresponds by retrieval -- this ** -- The ticket use management tool 335 remains and it asks for the count 3311 of use with which reduce one, remain with the count of effective, and a difference with the count of available indicates the count of available to be (ST3311). While sending this to the client means 31 as license challenge Challenge306 through the 3rd transceiver means 331 (ST3312), it sends also to the 3rd multistage hash means 336. Moreover, it sends to the license collating means 337 as it is by making the multistage hash value 3306 into the multistage hash value 3312.

[0090] On the other hand, in the client means 31, it is received by the 1st transceiver means 311, the count 3115 of use is taken out, and the license challenge

Challenge306 is sent to the multistage hash means 317 (ST3114). When the notice 3104 of use license procedure starting is given, the multistage hash means 317 A hash value 3113 is obtained from said secret storage means 316 (ST3115). The hash operation H of the number of stages equivalent to the difference of the count 3112 of effective and the count 3115 of use is performed to a hash value 3113 (ST3116). The multistage hash value 3116 of a result is sent to the license server means 33 as license challenge response Response307 through the 1st transceiver means 311 (ST3117).

[0091] As long as it, on the other hand, has tropism, the die length of a result, and random nature, since the third person whose hash operation H is insurance enough and who does not know Password PW and a random number R0 cannot calculate this multistage hash value 3116, it is shown that it is the valid user which gets to know Password PW by this multistage hash value 3116. Moreover, since many number of stages of the hash operation H in a multistage hash value are performed so that it went back in the past and the following multistage hash value is also incalculable from this multistage hash value 3116, there is also no need for encryption. In addition, generally a hash operation is made more nearly high-speed 100 or more times than a code operation, and if it is a suitable number of stages, it can process at a high speed rather than the case where a code is used.

[0092] On the other hand, in the license server means 33, it is received by the 3rd receiving means 331, the multistage hash value 3313 is taken out, and the license challenge response Response307 is sent to the 3rd multistage hash means 336 (ST3313). The 3rd multistage hash means 336 performs the hash operation H of the number of stages equivalent to the count 3311 of use to the multistage hash value 3313, and sends the secondary multistage hash value 3314 of a result to the license collating means 337 (ST3314). The license collating means 337 performs the coincidence judging with the multistage hash value 3312 and the secondary multistage hash value 3314 (ST3315, ST3316), and if it is truth, the client means 31 will receive the notice 3315 of license in delivery (ST3317) and the client means 31 through the 3rd transceiver means 331 as notice Result308 of license (ST3118). By this approach, the client means 31 can obtain use license to n times using the authentication ticket 305, without revealing Password PW to a third person including the license server means 33.

[0093] In addition, although considered as the configuration which calculates a multistage hash value in the client means 31 at every use license procedure in the above explanation, it is good also as a configuration which carries out precomputation of the multistage hash value of all number of stages at the time of acquisition of an authentication ticket, and is memorized for the secret storage means 316. In that case, the processing time for every use license procedure of what needs to use the mass Tampa-proof nature memory device as a secret storage means 316 can be shortened more.

[0094] Next, in the authentication system of the 4th operation gestalt shown in drawing 5 , the detailed example of a configuration and actuation of the authentication child addition means 328 at the time of using a message authorization code as an authentication child and the authentication child verification means 333 are explained with reference to drawing 7 and drawing 8 .

[0095] Self-identifier storage means 328A the identifier the authentication child addition means 328 indicates the authentication server itself to be as shown in drawing 7 was remembered to be, Data connection means 328B which connects data, and connection data hash means 328C which performs the hash operation h, Authentication child connection means 328F by which the authentication server means 31 and the license server means 32 connect an authentication child with server common key storage means 328D which memorizes the common server common key which it has as secret, and common key system cryptographer stage 328E which performs cipher processing of a common key system at data are provided.

[0096] This self-identifier storage means 328A consists of memory. Data connection means 328B can consist of logical circuits. Connection data hash means 328C consists of arithmetic circuits incorporating the algorithm of for example, the hash operation h. Even if the hash operation h is the same as the hash operation H, they may differ here. If server common key storage means 328D is the memory device which consisted of memory and had the Tamper-proof nature, in addition, it is good. Common key system cryptographer stage 328E consists of the arithmetic circuits or cipher-processing special purpose processors incorporating cryptographic algorithm. As cryptographic algorithm, DES, Triple DES, etc. can be used here, for example. Authentication child connection means 328F consist of logical circuits.

[0097] Moreover, authentication child separation means 333A into which the authentication child verification means 333 separates an authentication child from data as shown in drawing 8 , 2nd connection data hash means 333B which performs the hash operation h, 2nd server common key storage means 333C which memorizes the server common key with common authentication server means 31 and license server means 32 which it has as secret, It provides with 2nd common key system cryptographer stage 333D which performs cipher processing of a common key system, data separation means 333E which carries out division separation of the data division, publisher identifier collating means 333F which collate a publisher identifier, and comparison means 333G which carry out comparison verification of the message authorization code.

[0098] This authentication child separation means 333A consists of logical circuits. 2nd connection data hash means 333B, 2nd server common key storage means 333C, and 2nd common key system cryptographer stage 333D are constituted like 328C, 328D, and 328E in drawing 7 , respectively. Data separation means 333E consists of logical circuits. Publisher identifier collating means 333F consist of a memory circuit and a comparator circuit. Comparison means 333G are constituted by the

combination of a comparator circuit. In addition, each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or the computer program may be recorded on a program documentation medium in the format in which read is possible, and the configuration combined with the program documentation medium reader may realize.

[0099] Actuation of the authentication child addition means 328 constituted as mentioned above and the authentication child verification means 333 is explained. With the authentication child addition means 328, the identifier which shows the authentication server itself is first supplied to data connection means 328B as publisher identifier 328a from self-identifier storage means 328A. The count 3202 of effective and the server identifier 3203 which obtained data connection means 328B from the 2nd transceiver means 321, the multistage hash value 3210 obtained from the authentication collating means 326, and authentication -- a time check -- with the time stump 3211 obtained from the means 322 It arranges and connects in the sequence that the ticket identifier 3212 obtained from the ticket identifier generation means 327 and publisher identifier 328a obtained from self-identifier storage means 328A were able to be defined, and sends to connection data hash means 328C and authentication child connection means 328F as data-division 328b.

[0100] Connection data hash means 328C performs the hash operation h to data-division 328b, and sends hash value 328c of a result to common key system cryptographer stage 328E. Common key system cryptographer stage 328E obtains 328d of server common keys from server common key storage means 328D, uses this for a cryptographic key, enciphers hash value 328c, and sends it to authentication child connection means 328F as message authorization code 328e. Authentication child connection means 328F connect message authorization code 328e with data-division 328b, and output the authentication ticket data 3213.

[0101] Moreover, with the authentication child verification means 333, first, the authentication ticket data 3301 are inputted into authentication child separation means 333A, and it separates into message authorization code 333a and data-division 333b, and message authorization code 333a is sent to comparison means 333G, and data-division 333b is sent to 2nd connection data hash means 333B and data separation means 333E, respectively. 2nd connection data hash means 333B performs the hash operation h to data-division 333b, and sends hash value 333c of a result to 2nd common key system cryptographer stage 333D. 2nd common key system cryptographer stage 333D obtains 333d of server common keys from 2nd server common key storage means 333C, uses this for a cryptographic key, enciphers hash value 333c, and sends it to comparison means 333G as message authorization code 333for comparison e. Data separation means 333E sends also to publisher identifier collating means 333F about the publisher identifier 3308 while separating and outputting data-division 333b to a time stump 3302, the server identifier 3303, the ticket identifier 3305, the multistage hash value 3306, the count 3307 of effective, and

the publisher identifier 3308. The publisher identifier 3308 collates whether it is the identifier of an authentication server 32, and publisher identifier collating means 333F send 333f of collating results to comparison means 333G. Comparison means 333G output the verification result 3304 based on whether 333f of collating results shows coincidence, or message authorization code 333a and message authorization code 333e for a comparison are in agreement. Each that the verification result 3304 shows those without an error is the case of being in agreement.

[0102] Next, in the authentication system of the 4th operation gestalt of drawing 5, the configuration and actuation of the authentication child addition means 328 at the time of using a digital signature as an authentication child and the authentication child verification means 333 are explained with reference to drawing 9 and drawing 10. differing from drawing 7 in drawing 9 memorizes the public key system code private key of authentication server 32 self instead of server common key storage means 328D and common key system cryptographer stage 328E -- self--- it is in the point of having prepared public key system cryptographer stage 328H which perform cipher processing of private key storage means 328G and a public key system. self--- if it is the memory device which could use memory, for example and had the Tampa-proof nature as private key storage means 328G, in addition, it is good. As public key system cryptographer stage 328H, the arithmetic circuit or cipher-processing special purpose processor which incorporated cryptographic algorithm, for example can be used. As cryptographic algorithm, RSA, an elliptic curve cryptosystem, etc. can be used here, for example.

[0103] Moreover, differing from drawing 8 in drawing 10 prepares public key system decode means 333J which perform decode processing of server public key are recording means 333H which match the public key of the authentication server means 31 with a server identifier, and accumulate it one or more instead of 2nd server common key storage means 333C, 2nd common key system cryptographer stage 333D, and publisher identifier collating means 333F, and a public key system code, and it is in the point of having changed the connection between these. Server public key are recording means 333H are good also as what accumulates not only the authentication server means 32 but the public key of the license server means 33. As server public key are recording means 333H, a memory circuit can be used, for example, and if it is a mass memory device, in addition, it is good. As public key system decode means 333J, the arithmetic circuit or cipher-processing special purpose processor which incorporated the decode algorithm, for example can be used. It cannot be overemphasized that the decode algorithm corresponding to the cryptographic algorithm in public key system cryptographer stage 328H is used as a decode algorithm here. In addition, each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or the computer program may be recorded on a program documentation medium in the format in which read is possible, and the configuration combined with the program

documentation medium reader may realize.

[0104] Actuation of the authentication child addition means 328 constituted as mentioned above and the authentication child verification means 333 is explained. With the authentication child addition means 328, actuation of self-identifier storage means 328A, data connection means 328B, and connection data hash means 328C is the same as that of the case of drawing 7, data-division 328b is supplied to authentication child connection means 328F, and hash value 328c is supplied to public key system cryptographer stage 328H, respectively. public key system cryptographer stage 328H -- self-- 328f of self-private keys is obtained from private key storage means 328G, this is used for a cryptographic key, hash value 328c is enciphered, and it sends to authentication child connection means 328F as 328g of digital signatures. Authentication child connection means 328F connect 328g of digital signatures with data-division 328b, and output the authentication ticket data 3213.

[0105] Moreover, with the authentication child verification means 333, first, the authentication ticket data 3301 are inputted into authentication child separation means 333A, and it separates into 333g of digital signatures, and data-division 333b, and 333g of digital signatures is sent to public key system decode means 333J, and data-division 333b is sent to 2nd connection data hash means 333B and data separation means 333E, respectively. 2nd connection data hash means 333B performs the hash operation h to data-division 333b, and sends the hash value of 333h of a result to comparison means 333G. Data separation means 333E sends also to server public key are recording means 333H about the publisher identifier 3308 while separating and outputting data-division 333b to a time stamp 3302, the server identifier 3303, the ticket identifier 3305, the multistage hash value 3306, the count 3307 of effective, and the publisher identifier 3308. Server public key are recording means 333H send server public key 333j corresponding to the publisher identifier 3308 to public key system decode means 333J while the publisher identifier 3308 carries out retrieval collating of whether it is the identifier of the known authentication server 31 (or license server 32) and sends collating result 333i to comparison means 333G.

[0106] Public key system decode means 333J use server public key 333j for a decode key, decrypt 333g of digital signatures, and send them to comparison means 333G as hash value 333for comparison k. Comparison means 333G output the verification result 3304 based on whether collating result 333i shows coincidence or the hash value of 333h and hash value 333k for a comparison are in agreement. Each that the verification result 3304 shows those without an error is the case of being in agreement.

[0107] Thus, when an authentication system takes the configuration of this operation gestalt, even if a client side is low equipment of computation capacity, it becomes possible to perform use license processing by the practical processing time.

[0108] (Gestalt of the 5th operation) The 5th operation gestalt explains the block

configuration of each means to perform the concrete communication procedure and concrete it in the authentication system of the 3rd operation gestalt.

[0109] Drawing 11 is the protocol sequence diagram showing the protocol of the authentication system in the 5th operation gestalt. It is to differ from drawing 4 in drawing 11 with the client means 41 with a user interface, and an authentication server means 42 to perform user authentication, and the license server means 33 does not have a change. moreover The authentication challenge response Response401 minds a user interface. The point accompanied by the exclusive-OR result (a notation "@" shows EXCLUSIVE OR operation) of the result of having performed one step of hash operation H to connection by Password PW and the random number R0 which were inputted, and the random number S0 for authentication which the client means 41 generated in secrecy, The point that the hash result of an operation by which the authentication ticket 402 and Ticket 403 is accompanied is n steps of hash results of an operation to the random number S0 for authentication, It differs in that the hash result of an operation by which the license challenge response Response404 is accompanied is the hash operation of the n-k stage to the random number S0 for authentication.

[0110] By the above protocol sequences, the client means 41 can obtain use license to n times using the authentication ticket 402, and is not set even as the attack object for stealing the password PW by the inaccurate third person, since the authentication tickets 402 are contents unrelated to Password PW, without revealing Password PW to a third person including the license server means 33, but safety is more high.

[0111] It explains referring to the functional block diagram of drawing 12 about the configuration with such a protocol sequence of an authentication system.

[0112] Also in drawing 12, an authentication server means 42 to perform the client means 41 and user authentication with a user interface differs from drawing 5, and the license server means 33 does not have a change. Moreover, differing from the client means 31 of drawing 5 in the client means 41 establishes a random-number generation means 411 for authentication to generate a random number for every user authentication processing, and the 1st exclusive-OR means 412 which performs EXCLUSIVE OR operation for every bit, and it is in the point of having changed a part of connection. Moreover, differing from the authentication server means 32 of drawing 5 in the authentication server means 42 establishes the 2nd exclusive-OR means 422 which performs EXCLUSIVE OR operation for every 2nd 421 bit hash means which performs the hash operation H instead of the 2nd multistage hash means 325 and the authentication collating means 326, and the 2nd multistage hash means 423 which performs the hash operation H of the given number of stages, and it is in the point of having changed a part of connection. As a random-number generation means 411 for authentication, the arithmetic circuit which incorporated the random-number generation algorithm, for example, or the inverter which data-izes an electromagnetic

noise can be used. As 1st and 2nd exclusive-OR means 412 and 422, a logical circuit can be used, for example. As 2nd hash means 421, the arithmetic circuit which incorporated the algorithm of the hash operation H, for example can be used. The counter which counts the connection which feeds back an output, for example to the same arithmetic circuit as 421, and a number of stages as 2nd multistage hash means 423 can be added and constituted. In addition, each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or the computer program may be recorded on a program documentation medium in the format in which read is possible, and the configuration combined with the program documentation medium reader may realize.

[0113] It explains referring to drawing 13 about actuation of the authentication system constituted as mentioned above. Here, the case where authentication demand Authenticate Request301 is accompanied by the count n of authentication ticket effective is explained.

[0114] First, in the client means 41 and the authentication server means 42, actuation of the 1st, the 2nd transceiver means 311 and 321, the input means 312, the ticket maintenance means 314, the processing selection means 315, the authentication information storage means 323, and the random-number generation means 324 is the same as that of the case of drawing 5 and drawing 6. It is exchanged in authentication demand Authenticate Request301 and the authentication challenge Challenge302. In the client means 41 the notice 4101 of user authentication processing starting or the notice 3104 of use license procedure starting In the authentication server means 42, the count 4201 of effective, the server identifier 3203, a password 3204, the notice 4202 of a retrieval result, and the challenge random number 3206 are obtained. However, the point that the notice 4101 of user authentication processing starting is sent to said input means 312, the random-number generation means 411 for authentication, and the 1st exclusive-OR means 412, The point that the count 4201 of effective is sent to the 2nd multistage hash means 423 and the authentication child addition means 328, The point that the notice 4202 of a retrieval result is sent to the 2nd hash means 421, the random-number generation means 324, and the ticket identifier generation means 327, While the challenge random number 3206 is sent to the 2nd hash means 421, the points sent to the client means 41 through the 2nd transceiver means 321 differ.

[0115] Next, in the client means 41, if the notice 4101 of user authentication processing starting is given, the random-number generation means 411 for authentication will newly generate the random number 4102 for authentication used for attested certification on random and the secret reverse side, and will send it to the 1st exclusive-OR means 412 and secret storage means 316 (ST4101). The secret storage means 316 memorizes the random number 4102 for authentication in secrecy, and permits only predetermined access, i.e., the renewal of an addition in a user authentication procedure and the reference in a use license procedure, (ST4102). If

the notice 4101 of user authentication processing starting is given, between the hash values 4103 and the random numbers 4102 for authentication which were obtained from the hash means 313, the 1st exclusive-OR means 412 will perform EXCLUSIVE OR operation for every bit, and will send the disturbance hash value 4104 obtained as a result to the authentication server means 42 as authentication challenge response Response401 through the 1st transceiver means 311 (ST4103, ST4104).

[0116] On the other hand, in the authentication server means 42, it is received by the 2nd transceiver means 321, the disturbance hash value 4204 is taken out, and the authentication challenge response Response401 is sent to the 2nd exclusive-OR means 422 (ST4202). On the other hand, when the notice 4202 of a retrieval result shows owner **, the 2nd hash means 421 performs the hash operation H to connection by the password 3204 and the challenge random numbers 3206, and supplies the hash value 4203 of a result to the 2nd exclusive-OR means 422 (ST4201). The 2nd exclusive-OR means 422 performs EXCLUSIVE OR operation for every bit between the hash values 4203 and the disturbance hash values 4204 which were obtained from the 2nd hash means 421, and sends the random number 4205 for authentication obtained as a result to the 2nd multistage hash means 423 (ST4203). The 2nd multistage hash means 423 performs the hash operation H of a number of stages equivalent to the count 4201 of effective to the random number 4205 for authentication, and sends the multistage hash value 4206 of a result to the authentication child addition means 328 (ST4204).

[0117] the following and ticket identifier generation means 327 and authentication -- a time check -- actuation of a means 322 and the authentication child addition means 328, although it is the same as that of the case of drawing 4 and drawing 5. The point of using the notice 4202 of a retrieval result instead of the ticket identifier generation means 327 being as a result of [3209] collating, It differs in that the count 4201 of effective and the multistage hash value 4206 are used instead of the authentication child addition means 328 being the count 3202 of effective, and the multistage hash value 3210. The authentication ticket data 4207 of contents which are different in the authentication ticket data 3213 are obtained (ST4205), and it is sent to the client means 41 as an authentication ticket Ticket402 through the 2nd transceiver means 321.

[0118] On the other hand, in the client means 41, when it operates like the case where said 1st transceiver means 311 and said ticket maintenance means 314 are drawing 5 and drawing 6 and the notice 3104 of use license procedure starting is given, the authentication ticket Ticket403 is sent to the license server means 33 with the license demand Authorize Request, and the count 3112 of effective is supplied to the multistage hash means 317.

[0119] Actuation of the license server means 33 against this is the same as that of the case of drawing 5 and drawing 6, and the license challenge Challenge306 is returned.

[0120] On the other hand, in the client means 41, it operates like the case where said 1st transceiver means 311 and the multistage hash means 317 are drawing 5 and drawing 6 . However, it is the random number 4105 for authentication which is obtained from said secret storage means 316 (ST4105), and processing is performed to this. That is, the hash operation H of the number of stages with which the multistage hash means 317 is equivalent to the difference of the count 3112 of effective and the count 3115 of use is performed (ST4106), and the multistage hash value 4106 of a result is sent to the license server means 33 as license challenge response Response404 through the 1st transceiver means 311 (ST4107).

[0121] It is only that, as for the multistage hash value by which the license challenge response Response404 which the license server means 33 obtains by this is accompanied, and the multistage hash value by which the authentication ticket Ticket403 is accompanied, the candidates for a hash differ in the case of drawing 5 and drawing 6 , and the operation relation between the former and the latter is maintained. Therefore, actuation of the license server means 33 against this is the same as that of the case of drawing 5 and drawing 6 ; and it is good, the relation of two multistage hash values is checked, if it admits being just, the notice Result308 of license will be returned, and it is received in the client means 41. By this approach, without revealing Password PW to a third person including the license server means 33, Password PW of the client means 41 is unrelated, and it can obtain use license to n times using the higher authentication ticket 402 of safety.

[0122] In addition, although considered as the configuration which calculates a multistage hash value in the client means 41 at every use license procedure in the above explanation, it is good also as a configuration which carries out precomputation of the multistage hash value of all number of stageses at the time of acquisition of an authentication ticket, and is memorized for the secret storage means 316. In that case, the processing time for every use license procedure of what needs to use the mass Tampa-proof nature memory device as a secret storage means 316 can be shortened more.

[0123] Thus, when an authentication system takes the configuration of this operation gestalt, even if a client side is low equipment of computation capacity, it becomes possible to perform use license processing by the practical processing time. Moreover, since the collating information included in an authentication ticket becomes unrelated to user authentication information, possibility that user authentication information will be guessed disappears from an authentication ticket, and the authentication approach of a single sign-on mold and an authentication system with more high safety are obtained.

[0124] (Gestalt of the 6th operation) In the authentication system of the 6th operation gestalt, the authentication ticket with which the count of use was updated is sent to a client means with the notice of license from a license server.

[0125] Drawing 14 is the protocol sequence diagram showing the protocol of this

authentication system. In drawing 14 , the client means 51 and the license server means 53 differ from drawing 4 , and the authentication server means 32 does not have a change. Moreover, it differs in that the authentication ticket Ticket501 updated by the client means 51 with the notice Result308 of license from the license server 53 is sent.

[0126] Compared with the authentication ticket 305, as for this authentication ticket Ticket501, the following point is different.

[0127] That is, the $n+1$ -step hash result of an operation in the authentication ticket 305 is transposed to the $+1$ step of $n-k$ hash result of an operation (k is a count of use). The count n of effective in the authentication ticket 305 remains, and it is transposed to count $n-k$ of available. The time stamp TS 0 is transposed to the new time stamp TS k . The publisher identifier IID is transposed to the server identifier which shows license server 53 self. Furthermore, a new authentication child is added.

[0128] By this approach, the client means 51 can obtain use license to n times using the authentication ticket 304 or the updated authentication ticket 501, without revealing Password PW to a third person including the license server means 53.

Moreover, since the time stamp of an authentication ticket is updated each time, an expiration date can be set up shorter. Therefore, the period which can become a candidate for an attack by the inaccurate third person becomes short, and safety is more high. Moreover, since one step is available for the hash operation in the license server means 53, the response time in a use license procedure can be shortened.

[0129] It explains referring to drawing 15 about the configuration with such a protocol sequence of an authentication system.

[0130] In drawing 15 , the client means 51 and the license server means 53 differ from drawing 5 , and the authentication server means 32 does not have a change. Moreover, differing from the client means 31 of drawing 5 in the client means 51 has the ticket maintenance means 511 in the point of having enabled it to also hold the authentication ticket data 5101 of the authentication ticket Ticket501 from the license server means 53. Moreover, differing from the license server means 33 of drawing 5 in the license server means 53 establishes the 3rd hash means 532 which the ticket use management tool 531 shall remain, shall also output the count of available, and performs one step of hash operation H instead of the 3rd multistage hash means 336, the 2nd authentication child addition means 533 which generates and adds the authentication child to an authentication ticket newly establishes, and it is to the point of having changed a part of connection.

[0131] As this ticket maintenance means 511, the same configuration as the ticket maintenance means 314 can add and use connection. As a ticket use management tool 531, the same configuration as the ticket use management tool 335 can add and use connection. As 3rd hash means 532, the arithmetic circuit which incorporated the algorithm of the hash operation H, for example can be used. As 2nd authentication child addition means 533, the same configuration as the authentication child addition

means 328 can be used. In addition, each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or the computer program may be recorded on a program documentation medium in the format in which read is possible, and the configuration combined with the program documentation medium reader may realize.

[0132] It explains referring to drawing 16 about actuation of the authentication system constituted as mentioned above. Here, the case where authentication demand Authenticate Request301 is accompanied by the count n of authentication ticket effective is explained.

[0133] First, the actuation in the client means 51 and the authentication server means 32 is the same as that of the case of drawing 5 and drawing 6, a user authentication procedure is performed and, finally the authentication ticket Ticket304 is sent to the client means 51 from the authentication server means 32.

[0134] On the other hand, in the client means 51, the 1st transceiver means 311 operates like the case of drawing 5 and drawing 6, the count 3112 of effective is taken out from authentication ticket data, and the ticket maintenance means 511 is sent to the multistage hash means 317 while operating like drawing 5 and the ticket maintenance means 314 in the case of drawing 6 and sending the authentication ticket Ticket305 to the license server means 53 with the license demand Authorize Request.

[0135] on the other hand, the license server means 53 -- setting -- the 3rd transceiver means 331 and license -- a time check -- a means 332, the authentication child verification means 333, and the ticket effective judging means 334 operate like the case of drawing 5 and drawing 6, and supply the ticket identifier 3305, the multistage hash value 3306, the count 3307 of effective, the publisher identifier 3308, and the ticket effective notice 3310 to the ticket use management tool 531. The ticket use management tool 531 operates almost like drawing 5 and the ticket use management tool 335 in the case of drawing 6. Although the count 5301 of use is sent to the client means 51 as it is as license challenge Challenge306 through the 3rd transceiver means 331 at the license collating means 337 by making delivery and the multistage hash value 3306 into the multistage hash value 5302 Furthermore, it remains with a ticket identifier, the group 5303 of the count of available and a server identifier is outputted, and it sends to the 2nd authentication child addition means 533.

[0136] Actuation of the client means 51 against this is the same as that of the case of drawing 5 and drawing 6, and the license challenge response Response307 is returned to the license challenge Challenge306.

[0137] On the other hand, in the license server means 53, it is received by the 3rd transceiver means 331, the multistage hash value 5304 is taken out, and the license challenge response Response307 is sent to the 3rd hash means 532 and the 2nd authentication child addition means 533. The 3rd hash means 532 performs the hash

operation H to the multistage hash value 5304, and sends the secondary multistage hash value 5305 whose number of stages of a hash increased by one to the license collating means 337 (ST5301). The license collating means 337 performs the coincidence judging with the multistage hash value 5302 and the secondary multistage hash value 5305 (ST5302, ST3316), and sends the collating result 5307 to the 2nd authentication child addition means 533.

[0138] license -- a time check -- the means 322 has clocked current time and supplies the time stamp 5306 based on current time to the 2nd authentication child addition means 533. The 2nd authentication child addition means 533 connects the publisher identifier which remains with a ticket identifier and shows count [of available], group [of a server identifier] 5303, multistage hash value 5304, time stamp 5306, and license server 53 self. On the other hand, an authentication child is generated and added, and it considers as the authentication ticket data 5308 (ST5303), and sends to the client means 51 with the notice Result308 of license as an authentication ticket Ticket501 through the 3rd transceiver means 331 (ST5304). [0139] On the other hand, in the client means 51, it is received by the 1st transceiver means 311, and as authentication ticket data 5101, the authentication ticket Ticket501 is sent to said ticket maintenance means 511, is held (ST5101, ST5102), and is used in a next use license procedure.

[0140] Since, as for a decrease, the number of stages goes every [1] for every use license in the multistage hash value by which the authentication ticket 305 sent to the license server means 53 from the client means 51 by this is accompanied, with the license server means 53, the response time can be shortened that what is necessary is just to perform one step of hash operation. Moreover, since a time stamp is updated, it can set to the shortness of extent which can cover spacing of access to an expiration date, for example, 1 hour, and user convenience can raise safety, without making it fall. By this approach, the client means 31 can obtain use license in the shorter response time to n times using the higher authentication ticket 305 of safety, without revealing Password PW to a third person including the license server means 53.

[0141] In addition, although considered as the configuration which calculates a multistage hash value in the client means 51 at every use license procedure in the above explanation, it is good also as a configuration which carries out precomputation of the multistage hash value of all number of stageses at the time of acquisition of an authentication ticket, and is memorized for the secret storage means 316. In that case, the processing time for every use license procedure of what needs to use the mass Tampa-proof nature memory device as a secret storage means 316 can be shortened more.

[0142] Thus, in the authentication system of the gestalt of this operation, possibility of the unauthorized use by the third person can be made smaller, and the response time of use license can be shortened.

[0143] (Gestalt of the 7th operation) An authentication ticket can be used for the authentication system of the 7th operation gestalt in common to two or more license servers.

[0144] Drawing 17 is the protocol sequence diagram showing the protocol of this authentication system. In drawing 17, the client means 61, the authentication server means 62, and the license server means 63 differ from drawing 4, and it has added the authentication ticket management tool 64 further. moreover The authentication challenge response Response303 The authentication ticket shelf registration directions Registration601 accompanied by the ticket identifier TID and the server identifier SID which the carrier beam authentication server means 62 took out from authentication demand Authenticate Request301, and the count n of effective The point sent to the authentication ticket management tool 64, the point accompanied by the count k of use in the license demand Authorize Request602, The license demand Authorize Request602 And the authentication ticket Ticket305 The renewal directions Update603 of authentication ticket hysteresis accompanied by the ticket identifier TID and the server identifier SID which the carrier beam license server means 63 took out from the license demand Authorize Request602 and the authentication ticket 305, and the count k of use The point sent to the authentication ticket management tool 64, the point that the notice Reject606 of authentication ticket refusal is returned if needed to this, The point accompanied by the random number R_k generated so that it might differ each time instead of the license challenge Challenge604 being the count k of use, The points accompanied by the result of having carried out EXCLUSIVE OR operation with R_k to the result to which the license challenge response Response605 performed the hash operation H of +one step of $n-k$ to connection by Password PW and random numbers R_0 further differ.

[0145] Since it checks with the authentication ticket management tool 64 which the client means 61 could obtain use license to n times using the authentication ticket 304, sent the count k of use from the client means 61, without revealing Password PW to a third person including the license server means 63, and became independent in the license server means 63 by this approach, the authentication ticket 304 can be made available in common with two or more license server means 63.

[0146] It explains referring to drawing 18 about the configuration with this protocol sequence of an authentication system. Also in drawing 18, the client means 61, the authentication server means 62, and the license server means 63 differ from drawing 5, and it has added the authentication ticket management tool 64 further. Moreover, differing from the client means 31 of drawing 5 in the client means 61 forms the ticket maintenance management tool 611 which manages the count k of use instead of the ticket maintenance means 314 while holding an authentication ticket, and it establishes the 1st exclusive-OR means 612 which performs EXCLUSIVE OR operation for every bit, and is in the point of having changed a part of connection. Moreover, differing from the authentication server means 32 of drawing 5 in the

authentication server means 62 establishes a ticket registration directions means 621 to generate authentication ticket shelf registration directions data, and it is in the point of having changed a part of connection.

[0147] Moreover, differing from the license server means 33 of drawing 5 in the license server means 63 A renewal directions means 631 of a ticket to generate the renewal directions data of authentication ticket hysteresis while remaining with the ticket identifier of an authentication ticket and the count of effective, receiving the count of available and supplying each part is established instead of the ticket use management tool 335. The 2nd exclusive-OR means 633 which performs EXCLUSIVE OR operation for every 2nd 632 bit random-number generation means which generates a random number for every use license processing is established, and it is in the point of having changed a part of connection.

[0148] As this ticket maintenance management tool 611, the adder circuit which calculates the count of use is added to the same configuration as the ticket maintenance means 335, and it is constituted. As 1st and 2nd exclusive-OR means 612 and 633, a logical circuit can be used, for example. As a ticket registration directions means 621, a logical circuit can be used, for example. As a renewal directions means 631 of a ticket, a logical circuit can be used, for example. As 2nd random-number generation means 632, the same configuration as the random-number generation means 324 can be used. The combination of the arithmetic circuit and comparator circuit which collate various communication-interface equipments, the logical circuit which performs division association of data, and the count of use as an authentication ticket management tool 64, and a mass memory device can constitute. In addition, each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or the computer program may be recorded on a program documentation medium in the format in which read is possible, and the configuration combined with the program documentation medium reader may realize.

[0149] It explains referring to drawing 19 about actuation of the authentication system constituted as mentioned above. Here, the case where authentication demand Authenticate Request301 is accompanied by the count n of authentication ticket effective is explained.

[0150] First, the actuation in the client means 61 in a user authentication procedure and the authentication server means 62 is the same as that of the case of drawing 5 and drawing 6 almost, and, finally the authentication ticket Ticket304 is sent to the client means 61 from the authentication server means 62. However, in the client means 61, the ticket maintenance management tool 611 operates the ticket maintenance means 314 at this time. Moreover, the count 6201 of effective taken out from authentication demand Authenticate Request301 is sent also to a ticket registration directions means 621 besides the multistage hash means 325 and the authentication child addition means 328, a server identifier 6202 is sent also to a

ticket registration directions means 621 besides the authentication child addition means 328, and the ticket identifier 6203 generated with the ticket identifier generation means 327 is sent in an authentication server means 62 also to a ticket registration directions means 621 besides the authentication child addition means 328. [0151] The ticket registration directions means 621 connects the ticket identifier 6203, the server identifier 6202, and the count 6201 of effective, generates the authentication ticket shelf registration directions data 6204, and sends them to the authentication ticket management tool 64 as authentication ticket shelf registration directions Registration601 through the 2nd transceiver means 321 (ST6201). It investigates whether when the ticket list is managed and the authentication ticket shelf registration directions Registration601 are given, the authentication ticket management tool 64 which received this uses a ticket identifier, searches under a ticket list, and is already registered. If there is nothing corresponding, the group of the count of effective as a value which remains with a ticket identifier and the count of effective, and shows the count of available will be added to a ticket list, and will be memorized.

[0152] On the other hand, in the client means 61, it is received by the 1st transceiver means 311, the authentication ticket data 3110 are taken out, and the authentication ticket Ticket304 is sent to the ticket maintenance management tool 611. Match the ticket maintenance management tool 611 with the server identifier 3101, and it holds the authentication ticket data 3110. Remain and the count of effective taken out from authentication ticket data is managed to coincidence as a count of available (ST6101). When the notice 6101 of use license procedure starting is given, the 1st transceiver means 311 is minded for the authentication ticket data 3111. As an authentication ticket Ticket305 The 1st (ST6102) transceiver means 311 is minded for the count 6102 of use obtained by lengthening from the count of effective taken out from the authentication ticket after remaining and reducing the count of available one. Moreover, as license demand Authorize Request602 Delivery (ST6103) and the count 3112 of effective taken out from authentication ticket data are further sent to the license server means 63 at the multistage hash means 317.

[0153] On the other hand, in the license server means 63, it is received by the 3rd transceiver means 331 and the authentication ticket data 3301 are taken out, it is sent to the authentication child verification means 333, the count 6301 of use is taken out, and the authentication ticket Ticket305 and the license demand Authorize Request602 are sent to the renewal directions means 631 of a ticket (ST6301). license -- a time check -- a means 332, the authentication child verification means 333, and the ticket effective judging means 334 operate almost like the case of drawing 5 and drawing 6 , however the server identifier 6302 is sent also to the renewal directions means 631 of a ticket besides the ticket effective judging means 334, and the effective notice 6303 is sent to the renewal directions means 631 of a ticket, and the 2nd random-number generation means 632. if, as for the renewal

directions means 631 of a ticket, the effective notice 6303 is given -- the ticket identifier 3305, the server identifier 6302, and the count 6301 of use -- connecting -- the renewal directions data 6304 of authentication ticket hysteresis -- generating -- the 3rd transceiver means 331 -- minding -- as the renewal directions Update603 of authentication ticket hysteresis -- the authentication ticket management tool 64 -- sending (ST6302) -- it sends to the 3rd multistage hash means 336 as it is by making the count 6301 of use into the count 6306 of use. When the renewal directions Update603 of authentication ticket hysteresis are given, the authentication ticket management tool 64 Search under a ticket list using a ticket identifier, and the value which shows the corresponding count of effective It is confirmed that it is in agreement with the sum total with the count of use by which the corresponding value and the corresponding renewal directions Update603 of authentication ticket hysteresis which remain and show the count of available are accompanied. If right, the value which shows the count of remaining available under ticket list will be reduced one, and if not right, the notice Reject606 of authentication ticket refusal is returned. The notice 606 of authentication ticket refusal is sent to said renewal directions means 631 of a ticket as notice data 6305 of authentication ticket refusal through the 3rd transceiver means 331 in the license server means 63. Although the renewal directions means 631 of a ticket is sent to the license collating means 337 as it is by making the multistage hash value 3306 into the multistage hash value 3312, if the notice data 6305 of authentication ticket refusal are given, it will inhibit this. The 2nd random-number generation means 632 is sent to the client means 61 as license challenge Challenge604 through the 3rd transceiver means 331 while it will newly generate the challenge random number 6307 for data disturbance at random and will send it to the 2nd exclusive-OR means 633, if the effective notice 6303 is given (ST6303).

[0154] On the other hand, in the client means 61, it is received by the 1st transceiver means 311, the challenge random number 6103 is taken out, and the license challenge Challenge604 is sent to the 1st exclusive-OR means 612 (ST6104). When the notice 6101 of use license procedure starting is given, from said secret storage means 316, the multistage hash means 317 obtains a hash value 3113, performs the hash operation H of the number of stages which is equivalent to the difference of the count 3112 of effective, and the count 6102 of use at a hash value 3113, and sends the multistage hash value 6104 of a result to the 1st exclusive-OR means 612. When the notice 6101 of use license procedure starting is given, the 1st exclusive-OR means 612 performs EXCLUSIVE OR operation for every bit between the multistage hash value 6104 and the challenge random number 6103, generates the disturbance multistage hash value 6105, and sends it to the license server means 63 as license challenge response Response605 through the 1st transceiver means 311 (ST6105, ST6106). As long as it, on the other hand, has tropism, the die length of a result, and random nature, since the third person whose hash operation H is insurance enough

and who does not know Password PW, a random number R0, and a challenge random number cannot calculate this disturbance multistage hash value 6105, it is shown that it is the valid user which gets to know Password PW by this disturbance multistage hash value 6105. Moreover, since many number of stageses of the hash operation H in a multistage hash value are performed so that it went back in the past and the following multistage hash value is also incalculable from this multistage hash value 6104, there is also no need for encryption. In addition, generally a hash operation is made more nearly high-speed 100 or more times than a code operation, and if it is a suitable number of stages, it can process at a high speed rather than the case where a code is used.

[0155] On the other hand, in the license server means 63, it is received by the 3rd transceiver means 331, the disturbance multistage hash value 6308 is taken out, and the license challenge response Response605 is sent to the 2nd exclusive-OR means 633 (ST6304). The 2nd exclusive-OR means 633 performs EXCLUSIVE OR operation for every bit between the challenge random number 6307 and the disturbance multistage hash value 6308, obtains the multistage hash value 6309, and sends it to the 3rd multistage hash means 336 (ST6305). The 3rd multistage hash means 336 performs the hash operation of the number of stages equivalent to the count 6306 of use to the multistage hash value 6309, and sends the secondary multistage hash value 3314 of a result to the license collating means 337. The license collating means 337 operates like the case of drawing 5 and drawing 6, and the client means 61 receives the notice data 3315 of license in delivery and the client means 61 through the 3rd transceiver means 331 as notice Result308 of license. However, it is not this limitation when supply of the multistage hash value 3312 is inhibited by reception of the notice Reject606 of authentication ticket refusal (ST6306, ST6307). By this approach, the client means 61 can obtain use license to two or more license server means using the authentication ticket 305 to n times, without revealing Password PW to a third person including the license server means 63.

[0156] In addition, although considered as the configuration which calculates a multistage hash value in the client means 61 at every use license procedure in the above explanation, it is good also as a configuration which carries out precomputation of the multistage hash value of all number of stageses at the time of acquisition of an authentication ticket, and is memorized for the secret storage means 316. In that case, the processing time for every use license procedure of what needs to use the mass Tampa-proof nature memory device as a secret storage means 316 can be shortened more.

[0157] Thus, the authentication system of the high single sign-on mold of convenience which can use an authentication ticket in common to two or more license servers under the method with which an authentication ticket is not updated can consist of this operation gestalt.

[0158] (Gestalt of the 8th operation) The authentication system of the 8th operation

gestalt can carry out distributed management of the use of an authentication ticket.

[0159] Drawing 20 is the protocol sequence diagram showing the protocol of this authentication system. In drawing 20, the client means 71, the authentication server means 72, and the license server means 73 differ from drawing 14, and it has added the 2nd license server means 74 further. Moreover, the point accompanied by the count k of use in the license demand Authorize Request701, The license demand Authorize Request701 And the authentication ticket Ticket305 The authentication ticket hysteresis enquiry Inquiry702 accompanied by the ticket identifier TID and the server identifier SID which the carrier beam license server means 73 took out from the license demand Authorize Request701 and the authentication ticket 305, and the count k of use The point sent to the authentication server means 72 or the 2nd license server means 74, the point that the notice Reject705 of authentication ticket refusal is returned if needed to this, The point accompanied by the random number R_k generated so that it might differ each time instead of the license challenge Challenge703 being the count k of use, The points accompanied by the result of having carried out EXCLUSIVE OR operation with R_k to the result to which the license challenge response Response704 performed the hash operation H of +one step of $n-k$ to connection by Password PW and random numbers R_0 further differ.

[0160] By this approach, the client means 71, without revealing Password PW to a third person including the license server means 73 and the 2nd license server means 74 Use license can be obtained to n times using the authentication ticket 304 or the updated authentication ticket 501. In order to send and check the count k of use for the authentication server means 72 or the 2nd updated license server means 74 which the authentication ticket was published through the license server means 73 from the client means 71, The authentication ticket 304 can be made available in common with two or more license server means 73 and 74, and the traffic of check processing can be decentralized.

[0161] It explains referring to drawing 21 about the configuration with such a protocol sequence of an authentication system. Also in drawing 21, the client means 71, the authentication server means 72, and the license server means 73 differ from drawing 15, and it has added the 2nd license server means 74 further. Moreover, differing from the client means 51 of drawing 15 in the client means 71 forms the ticket maintenance management tool 711 which manages the count k of use instead of the ticket maintenance means 511 while holding an authentication ticket, and it establishes the 1st exclusive-OR means 712 which performs EXCLUSIVE OR operation for every bit, and is in the point of having changed a part of connection. Moreover, differing from the authentication server means 32 of drawing 15 in the authentication server means 72 forms the ticket issue management tool 721 which manages issue of an authentication ticket and is answered to enquiry, and it is in the point of having changed a part of connection. Moreover, differing from the license server means 53 of drawing 15 in the license server means 73 The renewal

management tool 731 of a ticket which manages renewal of an authentication ticket and is answered to enquiry while remaining with the ticket identifier of an authentication ticket and the count of effective, receiving the count of available and supplying each part is formed instead of the ticket use management tool 531. The 2nd exclusive-OR means 733 which performs EXCLUSIVE OR operation for every 2nd 732 bit random-number generation means which generates a random number for every use license processing is established, and it is in the point of having changed a part of connection. The 2nd license server means 74 has the same configuration as the license server means 73.

[0162] It can be used as a ticket maintenance management tool 711, being able to add the adder circuit which calculates the count of use to the same configuration as the ticket maintenance means 511. As 1st and 2nd exclusive-OR means 712 and 733, a logical circuit can be used, for example. The combination of the arithmetic circuit and comparator circuit which collate the logical circuit which performs division association of data, for example, and the count of use as a ticket issue management tool 721, and a mass memory device can constitute. The combination of the arithmetic circuit and comparator circuit which collate the logical circuit which performs division association of data, for example, and the count of use as a renewal management tool 731 of a ticket, and a mass memory device can constitute. As 2nd random-number generation means 732, the same configuration as the random-number generation means 324 can be used. In addition, each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or the computer program may be recorded on a program documentation medium in the format in which read is possible, and the configuration combined with the program documentation medium reader may realize.

[0163] It explains referring to drawing 22 about actuation of the authentication system constituted as mentioned above. Here, the case where authentication demand Authenticate Request301 is accompanied by the count n of authentication ticket effective is explained.

[0164] First, the actuation in the client means 71 in a user authentication procedure and the authentication server means 72 is the same as that of the case of drawing 15 and drawing 16 almost, and, finally the authentication ticket Ticket304 is sent to the client means 71 from the authentication server means 72. However, in the client means 71, the ticket maintenance management tool 711 operates the ticket maintenance means 511 at this time. Moreover, in the authentication server means 72, the count 7201 of effective taken out from authentication demand Authenticate Request301 is sent also to the ticket issue management tool 721 besides the multistage hash means 325 and the authentication child addition means 328, the server identifier 7202 is sent also to the ticket issue management tool 721 besides the authentication child addition means 328, and the ticket identifier 7203 generated with the ticket identifier generation means 327 is sent also to the ticket issue

management tool 721 besides the authentication child addition means 328. The ticket issue management tool 721 has managed the published ticket list, and the group of the count 7201 of effective as a value which remains with the ticket identifier 7203, the server identifier 7202, and the count 7201 of effective, and shows the count of available is added to a ticket list, and it memorizes it (ST7201).

[0165] On the other hand, in the client means 71, it is received by the 1st transceiver means 311, the authentication ticket data 3110 are taken out, and the authentication ticket Ticket304 is sent to said ticket maintenance management tool 711. Match said ticket maintenance management tool 711 with the server identifier 3101, and it holds the authentication ticket data 3110. Remain and the count of effective taken out from authentication ticket data is managed to coincidence as a count of available (ST7101). When the notice 7101 of use license procedure starting is given, the 1st transceiver means 311 is minded for the authentication ticket data 3111. As an authentication ticket Ticket305 The 1st (ST7102) transceiver means 311 is minded for the count 7102 of use obtained by lengthening from the count of effective taken out from the authentication ticket after remaining and reducing the count of available one.

Moreover, as license demand Authorize Request701 Delivery (ST7103) and the count 3112 of effective further taken out from authentication ticket data are sent to the license server means 73 at the multistage hash means 317, respectively.

[0166] On the other hand, in the license server means 73, it is received by the 3rd transceiver means 331 and the authentication ticket data 3301 are taken out, it is sent to the authentication child verification means 333, the count 7301 of use is taken out, and the authentication ticket Ticket305 and the license demand Authorize Request701 are sent to the renewal management tool 731 of a ticket (ST7301).

[0167] license -- a time check -- a means 332, the authentication child verification means 333, and the ticket effective judging means 334 operate almost like the case of drawing 15 and drawing 16 , however the server identifier 7302 is sent also to the renewal management tool 731 of a ticket besides the ticket effective judging means 334, and the effective notice 7303 is sent to the renewal management tool 731 of a ticket, and the 2nd random-number generation means 732. If the published ticket list is managed and the effective notice 7303 is given, the renewal management tool 731 of a ticket Connect the ticket identifier 3305, the server identifier 7302, and the count 7301 of use, and the authentication ticket hysteresis enquiry data 7304 are obtained. While sending the authentication ticket hysteresis enquiry Inquiry702 to the authentication server means 72 or the 2nd license server means 74 which the publisher identifier 3308 shows through the 3rd transceiver means 331 The group of the count 7301 of effective as a value which remains with the ticket identifier 3305, the server identifier 7302, and the count 7301 of effective, and shows the count of available is added to a ticket list, and is memorized (ST7302).

[0168] With the authentication server means 72 which received this, it is received by the 2nd transceiver means 321 and the authentication ticket hysteresis enquiry

Inquiry702 is sent to said ticket issue management tool 721 as authentication ticket hysteresis enquiry data 7205 containing a ticket identifier, a server identifier, and the count of use. Said ticket issue management tool 721 investigates whether it is in agreement with what the count of use taken out from the authentication ticket hysteresis enquiry data 7205 remained with the count of effective managed itself, and was added to the difference with the count of available one, and, in the case of an inequality, returns the notice data 7204 of authentication ticket refusal as notice Reject705 of authentication ticket refusal through the 2nd transceiver means 321. In addition, when the 2nd license server means 74 receives this, the role as said ticket issue management tool 721 with the same renewal management tool of a ticket is performed.

[0169] In the license server means 73, the notice 705 of authentication ticket refusal is sent to said renewal management tool 731 of a ticket as notice data 7305 of authentication ticket refusal through the 3rd transceiver means 331. Although said renewal management tool 731 of a ticket remains in the license collating means 337 with delivery and a ticket identifier as it is by making the multistage hash value 3306 into the multistage hash value 5302 and sends the group 5303 of the count of available, and a server identifier to the 2nd authentication child addition means 533, if the notice data 7305 of authentication ticket refusal are given, it will inhibit these. The 2nd random-number generation means 732 is sent to the client means 71 as license challenge Challenge703 through the 3rd transceiver means 331 while it will newly generate the challenge random number 7306 for data disturbance at random and will send it to the 2nd exclusive-OR means 733, if the effective notice 7303 is given (ST7303).

[0170] On the other hand, in the client means 71, it is received by the 1st transceiver means 311, the challenge random number 7103 is taken out, and the license challenge Challenge703 is sent to the 1st exclusive-OR means 712 (ST7104). When the notice 7101 of use license procedure starting is given, from said secret storage means 316, the multistage hash means 317 obtains a hash value 3113, performs the hash operation H of the number of stages which is equivalent to the difference of the count 3112 of effective, and the count 7102 of use at a hash value 3113, and sends the multistage hash value 7104 of a result to the 1st exclusive-OR means 712. When the notice 7101 of use license procedure starting is given, the 1st exclusive-OR means 712 performs EXCLUSIVE OR operation for every bit between the multistage hash value 7104 and the challenge random number 7103, generates the disturbance multistage hash value 7105, and sends it to the license server means 73 as license challenge response Response704 through the 1st transceiver means 311 (ST7105, ST7106). As long as it, on the other hand, has tropism, the die length of a result, and random nature, since the third person whose hash operation H is insurance enough and who does not know Password PW, a random number R0, and a challenge random number cannot calculate this disturbance multistage hash value 7105, it is shown that

it is the valid user which gets to know Password PW by this disturbance multistage hash value 7105. Moreover, since many number of stageses of the hash operation H in a multistage hash value are performed so that it went back in the past and the following multistage hash value is also incalculable from this multistage hash value 7104, there is also no need for encryption. In addition, generally a hash operation is made more nearly high-speed 100 or more times than a code operation, and if it is a suitable number of stages, it can process at a high speed rather than the case where a code is used.

[0171] On the other hand, in the license server means 73, it is received by the 3rd transceiver means 331, the disturbance multistage hash value 7307 is taken out, and the license challenge response Response704 is sent to the 2nd exclusive-OR means 733 (ST7304). The 2nd exclusive-OR means 733 performs EXCLUSIVE OR operation for every bit between the challenge random number 7306 and the disturbance multistage hash value 7307, obtains the multistage hash value 7308, and sends it to the 3rd hash means 532 (ST7305). The 3rd hash means 532 performs a hash operation to the multistage hash value 7308, and sends the secondary multistage hash value 5305 of a result to the license collating means 337. The license collating means 337 and the 2nd authentication child addition means 533 operate like the case of drawing 15 and drawing 16 , and send the authentication ticket data 5308 to the client means 71 as an authentication ticket Ticket501 through the 3rd transceiver means 331. However, it is not this limitation, when it remains with the multistage hash value 5302 and a ticket identifier by reception of the notice Reject705 of authentication ticket refusal and supply of the group 5303 of the count of available and a server identifier is inhibited (ST7306, ST7307).

[0172] On the other hand, in the client means 71, it is received by the 1st transceiver means 311, and as authentication ticket data 5101, the authentication ticket Ticket501 is sent to said ticket maintenance management tool 711, is held (ST7107, ST7108), and is used in a next use license procedure.

[0173] Since, as for a decrease, the number of stages goes every [1] for every use license in the disturbance multistage hash value by which the authentication ticket 305 sent to the license server means 73 from the client means 71 by this is accompanied, with the license server means 73, the response time can be shortened that what is necessary is just to perform one step of hash operation. Moreover, since a time stamp is updated, it can set to the shortness of extent which can cover spacing of access to an expiration date, for example, 1 hour, and user convenience can raise safety, without making it fall. Without revealing Password PW to a third person including the license server means 73 and 74, using the higher authentication ticket 305 of safety, to n times, the client means 71 can obtain use license in the shorter response time, is available in common at two or more license servers, and can decentralize the traffic of check processing by this approach. [of that authentication ticket]

[0174] In addition, although considered as the configuration which calculates a multistage hash value in the client means 71 at every use license procedure in the above explanation, it is good also as a configuration which carries out precomputation of the multistage hash value of all number of stageses at the time of acquisition of an authentication ticket, and is memorized for the secret storage means 316. In that case, the processing time for every use license procedure of what needs to use the mass Tampa-proof nature memory device as a secret storage means 316 can be shortened more.

[0175] Thus, distributed management of the use of an authentication ticket can be carried out by constituting an authentication system like this operation gestalt under the method with which an authentication ticket is updated. Therefore, one management resource can be lessened more.

[0176]

[Effect of the Invention] In this invention, the authentication approach of a single sign-on mold and authentication system which cannot need cipher processing in a client side, but can manage the use count of an authentication ticket easily, and can eliminate [1st] duplex use are obtained so that clearly from the above explanation.

[0177] The authentication approach of a single sign-on mold and authentication system which can communalize data processing of authentication presentation information and data processing of presentation information in not needing cipher processing in a client side for the 2nd in a user authentication procedure are obtained.

[0178] In what generates collating information to the 3rd by making into confidential information the random number for authentication which the client means generated, since the collating information which an authentication ticket includes becomes unrelated to user authentication information, even possibility that user authentication information will be guessed from an authentication ticket cannot be found, and the authentication approach of a single sign-on mold with more high safety and an authentication system are obtained.

[0179] By 4th on the other hand performing the irreversible operation of confidential information by the tropism hash operation, even if a client side is low equipment of computation capacity, the authentication approach of a single sign-on mold and authentication system which can perform use license processing by the practical processing time are obtained.

[0180] Since it is updated by the 5th in that by which a license server means updates the collating information on an authentication ticket etc. whenever an authentication ticket uses it, and especially a time stump is updated and the expiration date in an effective judging can be set up shorter, possibility of the unauthorized use by the third person can be made smaller, and the authentication approach of the single sign-on mold which can shorten the response time of use license further, and an authentication system are obtained.

[0181] In what formed the authentication ticket management tool which manages the

use count of an authentication ticket in the 6th, in the system by which an authentication ticket is not updated, since it becomes possible to use an authentication ticket in common to two or more license servers, the authentication approach of a single sign-on mold with more high convenience and an authentication system are obtained.

[0182] In that an authentication server means and a license server means remember the issue hysteresis of an authentication ticket to be, in the system by which an authentication ticket is updated, since the distributed management of the use of an authentication ticket can be carried out, the authentication approach of a single sign-on mold and authentication system which can lessen one management resource more are obtained by the 7th.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The conceptual diagram showing the outline of the authentication system in the gestalt of operation of the 1st of this invention,

[Drawing 2] The conceptual diagram showing the outline of the authentication system in the gestalt of operation of the 2nd of this invention,

[Drawing 3] The conceptual diagram showing the outline of the authentication system in the gestalt of operation of the 3rd of this invention,

[Drawing 4] The protocol sequence diagram of the authentication system in the gestalt of operation of the 4th of this invention,

[Drawing 5] The functional block diagram of the authentication system in the gestalt of operation of the 4th of this invention,

[Drawing 6] The flow Fig. showing actuation of the authentication system in the gestalt of operation of the 4th of this invention,

[Drawing 7] The detailed functional block diagram of the authentication child addition means at the time of using a message authorization code in the authentication system in the gestalt of operation of the 4th of this invention,

[Drawing 8] The detailed functional block diagram of the authentication child verification means at the time of using a message authorization code in the authentication system in the gestalt of operation of the 4th of this invention,

[Drawing 9] The detailed functional block diagram of the authentication child addition means at the time of using a digital signature in the authentication system in the gestalt of operation of the 4th of this invention,

[Drawing 10] The detailed functional block diagram of the authentication child verification means at the time of using a digital signature in the authentication system

in the gestalt of operation of the 4th of this invention,

[Drawing 11] The protocol sequence diagram of the authentication system in the gestalt of operation of the 5th of this invention,

[Drawing 12] The functional block diagram of the authentication system in the gestalt of operation of the 5th of this invention,

[Drawing 13] The flow Fig. showing actuation of the authentication system in the gestalt of operation of the 5th of this invention,

[Drawing 14] The protocol sequence diagram of the authentication system in the gestalt of operation of the 6th of this invention,

[Drawing 15] The functional block diagram of the authentication system in the gestalt of operation of the 6th of this invention,

[Drawing 16] The flow Fig. showing actuation of the authentication system in the gestalt of operation of the 6th of this invention,

[Drawing 17] The protocol sequence diagram of the authentication system in the gestalt of operation of the 7th of this invention,

[Drawing 18] The functional block diagram of the authentication system in the gestalt of operation of the 7th of this invention,

[Drawing 19] The flow Fig. showing actuation of the authentication system in the gestalt of operation of the 7th of this invention,

[Drawing 20] The protocol sequence diagram of the authentication system in the gestalt of operation of the 8th of this invention,

[Drawing 21] The functional block diagram of the authentication system in the gestalt of operation of the 8th of this invention,

[Drawing 22] The flow Fig. showing actuation of the authentication system in the gestalt of operation of the 8th of this invention,

[Drawing 23] The conceptual diagram showing the outline of the conventional authentication approach,

[Drawing 24] The protocol sequence diagram of the conventional authentication approach,

[Drawing 25] The functional block diagram of the conventional authentication approach,

[Drawing 26] It is the flow Fig. showing actuation of the conventional authentication approach.

[Description of Notations]

1, 11, 21, 31, 41, 51, 61, 71, 81 Client means

2, 12, 22, 32, 42, 62, 72, 82 Authentication server means

3, 33, 53, 63, 73, 83 License server means

4, 14, 24 Confidential information

5 7,803,805 Authentication ticket

6,804 Presentation information

8,806 Notice of license

13 23,801 Authentication presentation information
64 Authentication Ticket Management Tool
74 2nd License Server Means
311 1st Transceiver Means
312 811 Input means
313 Hash Means
314 Ticket Maintenance Means
316 Secret Storage Means
317 Multistage Hash Means
321 2nd Transceiver Means
322 Authentication -- Time Check -- Means
323 Authentication Information Storage Means
324 Random-Number Generation Means
325 2nd Multistage Hash Means
326 Authentication Collating Means
327 Ticket Identifier Generation Means
328 Authentication Child Addition Means
328A Self-identifier storage means
328B Data connection means
328C Connection data hash means
328D Server common key storage means
328E Common key system cryptographer stage
328F Authentication child connection means
328G Self-private key storage means
328H Public key system cryptographer stage
331 3rd Transceiver Means
332 License -- Time Check -- Means
333 Authentication Child Verification Means
333A Authentication child separation means
333B The 2nd connection data hash means
333C The 2nd server common key storage means
333D The 2nd common key system cryptographer stage
333E Data separation means
333F Publisher identifier collating means
333G Comparison means
333H Server public key are recording means
333J Public key system decode means
334 832 Ticket effective judging means
335 531 Ticket use management tool
336 3rd Multistage Hash Means
337 License Collating Means

411 Random-Number Generation Means for Authentication
412, 612, 712 1st exclusive-OR means
421 2nd Hash Means
422 2nd Exclusive-OR Means
423 2nd Multistage Hash Means
511 Ticket Maintenance Means
532 3rd Hash Means
533 2nd Authentication Child Addition Means
611 711 Ticket maintenance management tool
621 Ticket Registration Directions Means
631 Renewal Directions Means of Ticket
632 2nd Random-Number Generation Means
633 733 2nd exclusive-OR means
721 Ticket Issue Management Tool
731 Renewal Management Tool of Ticket
732 2nd Random-Number Generation Means
812 Session Key Decode Means
813 Certification -- Time Check -- Means
814 Certification Information Cryptographer Stage
821 Session Key Generation Means
822 Session Key Cryptographer Stage
823 Ticket Cryptographer Stage
831 Ticket Decode Means
833 Certification Information Decode Means
834 Certification Information Effective Judging Means
835 License Collating Means

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-222360

(P2000-222360A)

(43) 公開日 平成12年8月11日 (2000.8.11)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 1 7
12/14	3 2 0	12/14	3 2 0 C 5 B 0 5 8
13/00	3 5 4	13/00	3 5 4 Z 5 B 0 8 5
G 0 6 K 17/00		G 0 6 K 17/00	T 5 B 0 8 9
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 A 5 J 1 0 4
審査請求 未請求 請求項の数29 O L (全 48 頁)			

(21) 出願番号 特願平11-24446

(22) 出願日 平成11年2月1日 (1999.2.1)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 柴田 顕男

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 高山 久

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100099254

弁理士 役 昌明 (外3名)

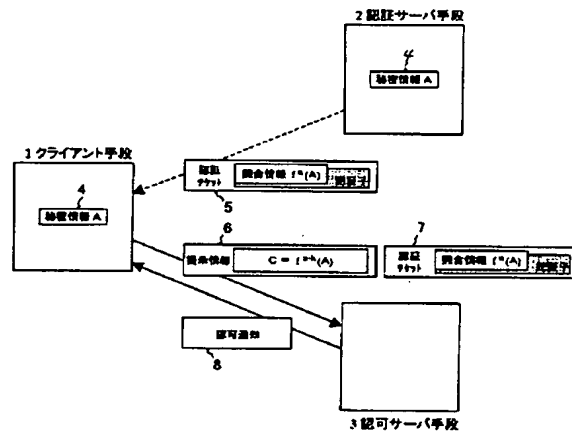
最終頁に続く

(54) 【発明の名称】 認証方法、認証システム及び認証処理プログラム記録媒体

(57) 【要約】

【課題】 1回のユーザ認証で複数回のアクセスを許可するシングルサインオン型認証において、少ない計算量で正当なアクセスを判別し、不正なアクセスを排除する。

【解決手段】 クライアント手段1と認証サーバ手段2とで秘密情報4を共有する。認証サーバ手段2は秘密情報4に不可逆演算 f を n 回行なった照合情報を含んだ認証チケット5を発行する。クライアント手段1はこの認証チケットとともに、秘密情報4に不可逆演算 f を $n-k$ 回行なった提示情報を認可サーバ手段3に示す。認可サーバ手段3はこの提示情報に不可逆演算 f を k 回行なって、照合情報と一致するかをチェックする。 k を1から n まで増加させることにより、過去の提示情報から次の提示情報を計算されることなく、最大 n 回のアクセスに認証チケット5が使用できる。



【特許請求の範囲】

【請求項1】 認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムにおいて、有効回数が n (n は正整数)である認証チケットを保持し、これを示して利用認可を求めるクライアント手段と、これを受けて前記クライアント手段に提示情報を要求し前記認証チケットと照合して利用を認可する認可サーバ手段とを具備し、前記認証チケットは、チケット識別子と照合情報と有効回数とを含み、且つ、認証子が付与されており、前記照合情報は、前記認証サーバ手段と前記クライアント手段とが共有する秘密情報に所定の不可逆演算を n 回施したものであり、前記認証チケットの使用回数が k (k は n 以下の正整数)であるときの前記提示情報は、前記秘密情報に前記所定の不可逆演算を $n-k$ 回施したものであることを特徴とする認証システム。

【請求項2】 前記認証サーバ手段が、ユーザ認証情報を管理し、前記クライアント手段との間でユーザ認証手順を実行して前記認証チケットを発行することを特徴とする請求項1に記載の認証システム。

【請求項3】 前記認証サーバ手段が、ユーザ認証手順において乱数を生成し、これを示して前記クライアント手段に認証提示情報を要求し、前記秘密情報は、前記ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を1回以上施したものであり、前記認証提示情報は、前記秘密情報に前記所定の不可逆演算を n 回施したものであることを特徴とする請求項2に記載の認証システム。

【請求項4】 前記認証サーバ手段が、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求し、前記認証提示情報が、前記ユーザ認証情報及び前記乱数との連結に前記所定の不可逆演算を1回以上施したものと前記クライアント手段が生成した認証用乱数との排他的論理和演算結果であり、前記秘密情報が、前記認証提示情報から逆算される前記認証用乱数であることを特徴とする請求項2に記載の認証システム。

【請求項5】 前記ユーザ認証情報が、ユーザにより入力されるパスワードであることを特徴とする請求項2から4のいずれかに記載の認証システム。

【請求項6】 前記ユーザ認証情報が、秘密裏に保持された共通鍵方式暗号鍵であることを特徴とする請求項2から4のいずれかに記載の認証システム。

【請求項7】 前記認証子が、メッセージ認証コードであることを特徴とする請求項1から6のいずれかに記載の認証システム。

【請求項8】 前記認証子が、デジタル署名であること

を特徴とする請求項1から6のいずれかに記載の認証システム。

【請求項9】 前記所定の不可逆演算が、方向性ハッシュ演算であることを特徴とする請求項1から8のいずれかに記載の認証システム。

【請求項10】 前記認証チケットが、サーバ識別子を含むことを特徴とする請求項1から9のいずれかに記載の認証システム。

【請求項11】 前記認証チケットが、発行日時を含むことを特徴とする請求項1から10のいずれかに記載の認証システム。

【請求項12】 前記認証チケットが、発行者識別子を含み、前記認可サーバ手段が、利用認可するとともに前記認証チケットの照合情報と有効回数と発行日時と発行者識別子と認証子とを更新し、前記照合情報が、前記秘密情報に前記所定の不可逆演算を $n-k$ 回施したものに更新され、前記有効回数が $n-k$ に更新されることを特徴とする請求項11に記載の認証システム。

【請求項13】 前記認可サーバ手段が、前記認証チケットの使用回数を管理しており、これを示して提示情報を要求することを特徴とする請求項1から12のいずれかに記載の認証システム。

【請求項14】 前記クライアント手段が、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めることを特徴とする請求項1から12のいずれかに記載の認証システム。

【請求項15】 複数の前記認可サーバ手段と、前記認証チケットの使用回数を管理する認証チケット管理手段とを備えており、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認証サーバ手段は、前記認証チケットを発行するとともに前記認証チケット管理手段に前記認証チケットの発行登録を指示し、前記認可サーバ手段は、前記認証チケットの提示を受けて前記認証チケット管理手段に前記認証チケットの履歴更新を指示し、前記認証チケット管理手段より拒絶通知を受けた場合には利用認可しないことを特徴とする請求項1から11のいずれかに記載の認証システム。

【請求項16】 前記認可サーバ手段を複数備え、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認証サーバ手段は、前記認証チケットを発行するとともに発行履歴を記憶し、前記認可サーバ手段は、前記認証チケットを更新するとともに更新履歴を記憶し、前記認証チケットの提示を受けて前記認証チケットの発行者識別子が示す前記認証サーバ手段または前記認可サーバ手段に前記認証チケットの履歴を照会し、前記認証サーバ手段または前記認可サーバ手段より拒絶通知を受けた場合には利用認可しない

ことを特徴とする請求項12に記載の認証システム。

【請求項17】 前記認可サーバ手段は、利用認可手順において乱数を生成し、これを示して提示情報を要求するものであり、前記認証チケットの使用回数が k であるときの前記提示情報は前記秘密情報に前記所定の不可逆演算を $n-k$ 回施したものと前記乱数との排他的論理和演算結果であることを特徴とする請求項14から16のいずれかに記載の認証システム。

【請求項18】 認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムにおいて、前記クライアント手段が、ユーザ識別子とユーザ認証情報とサーバ識別子と認証チケットの有効回数の入力を得る入力手段と、前記認証サーバ手段より認証チケットを得て保持し、前記認可サーバ手段に提示するチケット保持手段と、前記チケット保持手段より認証チケットの有無情報を得て処理を選択する処理選択手段と、前記入力手段よりユーザ認証情報を得るとともに前記認証サーバ手段より乱数を得て、これらの連結にハッシュ演算を施すハッシュ手段と、前記ハッシュ手段より得たハッシュ値を秘密裏に記憶する機密記憶手段と、前記機密記憶手段よりハッシュ値を取り出して、ユーザ認証手順においては前記入力手段より有効回数 n (n は正整数)を得て、 n 段のハッシュ演算を施して得た多段ハッシュ値を前記認証サーバ手段に送り、利用認可手順においては前記認可サーバ手段より利用回数 k (k は n 以下の正整数)を得て、 $n-k$ 段のハッシュ演算を施して得た多段ハッシュ値を前記認可サーバ手段に送る多段ハッシュ手段とを具備し、前記認証サーバ手段が、ユーザ認証情報が蓄積された認証情報蓄積手段と、乱数を生成して前記クライアント手段に送る乱数生成手段と、前記認証情報蓄積手段より得たユーザ認証情報と前記乱数生成手段で生成した乱数との連結に $n+1$ 段のハッシュ演算を行なう第2の多段ハッシュ手段と、前記クライアント手段より得た多段ハッシュ値を前記第2の多段ハッシュ手段で得た多段ハッシュ値と照合する認証照合手段と、有効なチケット識別子を生成するチケット識別子生成手段と、時刻を計時し時刻情報を出力する認証計時手段と、前記チケット識別子生成手段より得たチケット識別子、前記認証照合手段より得た多段ハッシュ値、前記クライアント手段より得たサーバ識別子及び有効回数、前記認証計時手段より得た時刻情報に基づくタイムスタンプ、並びに認証サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送る認証子付加手段とを具備し、前記認可サーバ手段が、前記クライアント手段より得た認証チケットの認証子を検証する認証子検証手段と、時

刻を計時し時刻情報を出力する認可計時手段と、サーバ識別子の妥当性及びタイムスタンプと前記認可計時手段より得た時刻情報との差の有効性をチェックするチケット有効判定手段と、認証チケットのチケット識別子と利用回数と残り利用可能回数とを管理するチケット利用管理手段と、前記チケット利用管理手段より利用回数 k を得て、前記クライアント手段より得た多段ハッシュ値に k 段のハッシュ演算を施して得た二次多段ハッシュ値を出力する第3の多段ハッシュ手段と、前記チケット利用管理手段より得た多段ハッシュ値と前記第3の多段ハッシュ手段より得た二次多段ハッシュ値とを照合する認可照合手段とを具備することを特徴とする認証システム。

【請求項19】 前記認証子付加手段が、サーバ間で共有する共通鍵方式暗号鍵を記憶するサーバ共通鍵記憶手段と、自識別子を記憶する自識別子記憶手段と、チケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と前記自識別子記憶手段より得た発行者識別子とを連結するデータ連結手段と、前記データ連結手段より得た連結データにハッシュ演算を施す連結データハッシュ手段と、前記サーバ共通鍵記憶手段より得た共通鍵方式暗号鍵を用いて前記連結データハッシュ手段より得たハッシュ値を暗号化して認証子とする共通鍵方式暗号手段と、前記データ連結手段より得た連結データと前記共通鍵方式暗号手段より得た認証子とを連結する認証子連結手段とを具備し、前記認証子検証手段が、サーバ間で共有する共通鍵方式暗号鍵を記憶する第2のサーバ共通鍵記憶手段と、認証チケットを連結データと認証子とに分離する認証子分離手段と、前記認証子分離手段より得た連結データをチケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と発行者識別子とに分離するデータ分離手段と、前記認証子分離手段より得た連結データにハッシュ演算を施す第2の連結データハッシュ手段と、前記第2のサーバ共通鍵記憶手段より得た共通鍵方式暗号鍵を用いて前記第2の連結データハッシュ手段より得たハッシュ値を暗号化して比較用認証子とする第2の共通鍵方式暗号手段と、前記データ分離手段より得た発行者識別子が有効なサーバ識別子であることをチェックする発行者識別子照合手段と、前記発行者識別子照合手段より得た照合結果が有効を示す場合に前記認証子分離手段より得た認証子と前記第2の共通鍵方式暗号手段より得た比較用認証子とを比較して結果を出力する比較手段とを具備することを特徴とする請求項18に記載の認証システム。

【請求項20】 前記認証子付加手段が、認証サーバの公開鍵方式暗号秘密鍵を秘密裏に記憶する自秘密鍵記憶手段と、自識別子を記憶する自識別子記憶手段と、チケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と前記自識別子記憶手段より得た発行者識別子とを連結するデータ連結手段と、前記データ連

結手段より得た連結データにハッシュ演算を施す連結データハッシュ手段と、前記自秘鍵記憶手段より得た公開鍵方式暗号秘鍵を用いて前記連結データハッシュ手段より得たハッシュ値を暗号化して認証子とする公開鍵方式暗号手段と、前記データ連結手段より得た連結データと前記公開鍵方式暗号手段より得た認証子とを連結する認証子連結手段とを具備し、

前記認証子検証手段が、認証チケットを連結データと認証子とに分離する認証子分離手段と、前記認証子分離手段より得た連結データをチケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と発行者識別子とに分離し出力するデータ分離手段と、前記認証子分離手段より得た連結データにハッシュ演算を施す第2の連結データハッシュ手段と、有効なサーバの公開鍵方式暗号公開鍵が蓄積され前記データ分離手段より得た発行者識別子に対応する公開鍵方式暗号公開鍵を出力するサーバ公開鍵蓄積手段と、前記サーバ公開鍵蓄積手段より得た公開鍵方式暗号公開鍵を用いて前記認証子分離手段より得た認証子を復号し比較用ハッシュ値とする公開鍵方式復号手段と、前記連結データハッシュ手段より得たハッシュ値と前記公開鍵方式復号手段より得た比較用ハッシュ値とを比較して結果を出力する比較手段とを具備することを特徴とする請求項18に記載の認証システム。

【請求項21】 前記クライアント手段が、認証乱数生成手段と第1の排他的論理和手段とを具備し、前記認証用乱数生成手段は、ユーザ認証手順において認証用乱数を生成し、前記第1の排他的論理和手段は、ユーザ認証手順において前記認証用乱数生成手段より得た認証用乱数と前記ハッシュ手段より得たハッシュ値との排他的論理和演算を行なって得た攪乱ハッシュ値を前記認証サーバ手段に送り、前記機密記憶手段は、前記認証用乱数生成手段より得た認証用乱数を秘密裏に記憶し、前記多段ハッシュ手段は、前記機密記憶手段より認証用乱数を取り出して、利用認可手順において前記認可サーバ手段より利用回数 k を得て、 $n-k$ 段のハッシュ演算を施して得た多段ハッシュ値を前記認可サーバ手段に送り、前記認証サーバ手段が、前記認証照合手段に代わり第2のハッシュ手段及び第2の排他的論理和手段を具備し、前記第2のハッシュ手段は、前記認証情報蓄積手段より得たユーザ認証情報と前記乱数生成手段で生成した乱数との連結にハッシュ演算を施し、前記第2の排他的論理和手段は、前記第2のハッシュ手段より得たハッシュ値と前記クライアント手段より得た攪乱ハッシュ値との排他的論理和演算を行なって認証用乱数を取得し、前記第2の多段ハッシュ手段は、前記第2の排他的論理和手段より得た認証用乱数に n 段のハッシュ演算を行ない、前記認証子付加手段は、前記チケット識別子生成手段より得たチケット識別子、前記第2の多段ハッシュ手段より得た多段ハッシュ値、前記クライアント手段より得たサ

ーバ識別子及び有効回数、前記認証計時手段より得た時刻情報に基づくタイムスタンプ、並びに認証サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送ることを特徴とする請求項18から20のいずれかに記載の認証システム。

【請求項22】 前記認可サーバ手段が、前記第3の多段ハッシュ手段に代わり第3のハッシュ手段及び第2の認証子付加手段を具備し、前記第3のハッシュ手段は、前記クライアント手段より得た多段ハッシュ値にハッシュ演算を施して得た二次多段ハッシュ値を出力し、前記認可照合手段は、前記チケット利用管理手段より得た多段ハッシュ値と前記第3のハッシュ手段より得た二次多段ハッシュ値とを照合し、前記第2の認証子付加手段は、前記チケット利用管理手段より得たチケット識別子、サーバ識別子及び残り利用回数、前記クライアント手段より得た多段ハッシュ値、前記認可計時手段より得た時刻情報に基づくタイムスタンプ、並びに認可サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送ることを特徴とする請求項18から21のいずれかに記載の認証システム。

【請求項23】 1つ以上の認可サーバ手段と、認証チケットの発行及び利用状況を管理する認証チケット管理手段とを具備し、前記認証チケット管理手段が、前記認証サーバ手段より得た認証チケット発行登録指示をもとにチケット識別子と有効回数と残り利用回数との組を管理して、前記認可サーバ手段より得た認証チケット履歴更新指示との整合性をチェックし、不整合の場合には前記認可サーバ手段に認証チケット拒絶通知を送り、前記認証サーバ手段が、チケット登録指示手段を具備し、前記チケット登録指示手段は、前記チケット識別子生成手段より得たチケット識別子と前記クライアント手段より得たサーバ識別子及び有効回数とから認証チケット発行登録指示を生成して前記認証チケット管理手段に送り、前記クライアント手段が、前記チケット保持手段に代わるチケット保持管理手段と、第1の排他的論理和手段とを具備し、前記チケット保持管理手段は、前記認証サーバ手段より認証チケットを得て保持するとともに利用回数を管理して、前記認可サーバ手段にそれらを提示し、前記多段ハッシュ手段は、前記機密記憶手段よりハッシュ値を取り出して、ユーザ認証手順においては n 段のハッシュ演算を施して得た多段ハッシュ値を前記認証サーバ手段に送り、利用認可手順においては前記チケット保持管理手段より得た利用回数 k を得て、 $n-k$ 段のハッシュ演算を施して得た多段ハッシュ値を前記第1の排他的論理和手段に送り、前記第1の排他的論理和手段は、前記多段ハッシュ手段より得た多段ハッシュ値と前記認可サーバ手段より得た乱数との排他的論理和演算を行な

って結果の攪乱多段ハッシュ値を前記認可サーバ手段に送り、

前記認可サーバ手段が、チケット利用管理手段に代わるチケット更新指示手段と、第2の乱数生成手段と、第2の排他的論理和手段とを具備し、前記チケット更新指示手段は、前記チケット有効判定手段より得た判定結果が有効を示す場合に前記認証子検証手段より得たチケット識別子及びサーバ識別子と前記クライアント手段より得た利用回数とから認証チケット履歴更新指示を生成して前記認証チケット管理手段に送り、前記認証チケット管理手段より認証チケット拒絶通知が返されなかった場合に前記クライアント手段より得た利用回数 k と前記認証子検証手段より得た多段ハッシュ値とを出力し、前記第2の乱数生成手段は、乱数を生成して前記クライアント手段及び前記第2の排他的論理和手段に送り、前記第2の排他的論理和手段は、前記第2の乱数生成手段より得た乱数と前記クライアント手段より得た攪乱多段ハッシュ値との排他的論理和演算を行なって多段ハッシュ値を取得し、前記第3の多段ハッシュ手段は、前記第2の排他的論理和手段より得た多段ハッシュ値に k 段のハッシュ演算を施して得た二次多段ハッシュ値を出力し、前記認証チケット管理手段は、前記認証サーバ手段より得た認証チケット発行登録指示をもとにチケット識別子と有効回数と残り利用回数との組を管理し、前記認可サーバ手段より得た認証チケット履歴更新指示との整合性をチェックし、不整合の場合には前記認可サーバ手段に認証チケット拒絶通知を送ることを特徴とする請求項18から21のいずれかに記載の認証システム。

【請求項24】 認可サーバ手段を1つ以上具備し、前記認証サーバ手段が、チケット発行管理手段を具備し、前記チケット発行管理手段は、前記チケット識別子生成手段より得たチケット識別子と前記クライアント手段より得たサーバ識別子及び有効回数とを管理し、前記認可サーバ手段より得たチケット利用照会をもとにチケット識別子を検索して利用回数の整合性をチェックし、不整合の場合には前記認可サーバ手段に認証チケット拒絶通知を送り、前記クライアント手段が、前記チケット保持手段に代わるチケット保持管理手段と、第1の排他的論理和手段とを具備し、前記チケット保持管理手段は、前記認証サーバ手段より認証チケットを得て保持するとともに利用回数を管理して、前記認可サーバ手段にそれらを提示し、前記多段ハッシュ手段は、前記機密記憶手段よりハッシュ値を取り出して、ユーザ認証手順においては n 段のハッシュ演算を施して得た多段ハッシュ値を前記認証サーバ手段に送り、利用認可手順においては前記チケット保持管理手段より得た利用回数 k を得て、 $n-k$ 段のハッシュ演算を施して得た多段ハッシュ値を前記第1の排他的論理和手段に送り、前記第1の排他的論理和手段は、前記多段ハッシュ手段より得た多段ハッシュ値と前記認

可サーバ手段より得た乱数との排他的論理和演算を行なって結果の攪乱多段ハッシュ値を前記認可サーバ手段に送り、

前記認可サーバ手段が、前記チケット利用管理手段に代わるチケット更新管理手段と、第2の乱数生成手段及び第2の排他的論理和手段とを具備し、前記チケット更新管理手段は、前記チケット有効判定手段より得た判定結果が有効を示す場合に前記認証子検証手段より得たチケット識別子及びサーバ識別子と前記クライアント手段より得た利用回数とからチケット利用照会を生成し、発行者識別子が示す前記認証サーバ手段または第2の認可サーバ手段に対して送り、前記認証サーバ手段または前記第2の認可サーバ手段より認証チケット拒絶通知が返されなかった場合に、前記クライアント手段より得た利用回数と前記認証子検証手段より得た多段ハッシュ値とを出力するとともに、チケット識別子、サーバ識別子及び残り利用回数を管理して、前記第2の認可サーバ手段よりチケット利用照会を受けた場合に利用回数の整合性をチェックし、不整合の場合には前記第2の認可サーバ手段に認証チケット拒絶通知を送り、前記第2の乱数生成手段は、乱数を生成して前記クライアント手段及び前記第2の排他的論理和手段に送り、前記第2の排他的論理和手段は、前記第2の乱数生成手段より得た乱数と前記クライアント手段より得た攪乱多段ハッシュ値との排他的論理和演算を行なって多段ハッシュ値を取得し、前記第2のハッシュ手段は、前記第2の排他的論理和手段より得た多段ハッシュ値にハッシュ演算を施して得た二次多段ハッシュ値を出力し、前記第2の認証子付加手段は、前記チケット管理手段より得たチケット識別子、サーバ識別子及び残り利用回数、前記第2の排他的論理和手段より得た多段ハッシュ値、前記認可計時手段より得た時刻情報に基づくタイムスタンプ、並びに認可サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送ることを特徴とする請求項22に記載の認証システム。

【請求項25】 認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムの認証方法において、

認証サーバ手段からクライアント手段に、認証サーバ手段とクライアント手段とが共有する秘密情報に所定の不可逆演算を n (n は正整数)回施した照会情報を含む、有効回数が n である認証チケットを発行し、クライアント手段は、前記認証チケットを認可サーバ手段に示して利用認可を求め、認可サーバ手段の提示情報の要求に対して、クライアント手段は、前記認証チケットの使用回数が k (k は n 以下の正整数)であるとき、前記秘密情報に前記所定の不可逆演算を $n-k$ 回施した演算結果を

前記提示情報として提示し、認可サーバ手段は、前記提示情報に前記所定の不可逆演算を k 回施し、その演算結果と前記照合情報との一致を識別することを特徴とする認証方法。

【請求項26】 認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムの認証方法において、

認証サーバ手段からクライアント手段に、認証サーバ手段とクライアント手段とが共有する秘密情報に所定の不可逆演算を n (n は正整数)回施した照合情報を含む、有効回数が n である認証チケットを発行し、クライアント手段は、前記認証チケットを認可サーバ手段に示して利用認可を求め、認可サーバ手段の提示情報の要求に対して、クライアント手段は、前記認証チケットの使用回数が k (k は n 以下の正整数)であるとき、前記秘密情報に前記所定の不可逆演算を $n-k$ 回施した演算結果を前記提示情報として提示し、認可サーバ手段は、前記提示情報に前記所定の不可逆演算を1回施し、その演算結果と前記照合情報との一致を識別するとともに、前記認証チケットに含まれる照合情報を前記秘密情報に前記所定の不可逆演算を $n-k$ 回施した演算結果に更新することを特徴とする認証方法。

【請求項27】 前記認証サーバ手段が、認証チケットを要求するクライアント手段に乱数を示して認証提示情報を要求し、クライアント手段は、ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を $n+1$ 回施した演算結果を前記認証提示情報として提示し、認証サーバ手段は、保持しているユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を $n+1$ 回施して、その演算結果と前記認証提示情報との一致を確認すると、前記ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を1回施した演算結果を前記秘密情報として、これに所定の不可逆演算を n (n は正整数)回施した前記照合情報を含む認証チケットを発行することを特徴とする請求項25または26に記載の認証方法。

【請求項28】 前記認証サーバ手段が、認証チケットを要求するクライアント手段に乱数を示して認証提示情報を要求し、クライアント手段は、ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を1回以上施したものとクライアント手段が生成した認証用乱数との排他的論理和演算結果を前記認証提示情報として提示し、認証サーバ手段は、保持しているユーザ認証情報と前記乱数とを用いて前記認証提示情報から前記認証用乱数を逆算し、前記認証用乱数を前記秘密情報として、これに所定の不可逆演算を n (n は正整数)回施した前記照合情報を含む認証チケットを発行することを特徴とする請求項25または26に記載の認証方法。

【請求項29】 請求項1から24のいずれかに記載の認証システムで実行される認証方法または請求項25から28のいずれかに記載の認証方法の処理プログラムを、電子計算機が読取り可能な形式で記録した、認証処理プログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、クライアント装置がサーバ装置にアクセスすることの妥当性を判断する1回の処理をもって複数回のアクセスを許可する、シングルサインオン型の認証方法及び認証システムに関し、特に、クライアント装置での暗号処理を不要にし、計算処理能力が低い装置でも処理できるようにしたものである。

【0002】

【従来の技術】近年、デジタル通信技術の発達にともない、ネットワークを介して接続されたサーバ装置及びクライアント装置から構成されるサーバ・クライアント型システムが一般的なものとなって来た。そのようなサーバ・クライアント型システムにおいては、クライアント装置及びそのユーザがサーバ装置にアクセスする正当な権限を有することを確認し、不正なアクセスが行なわれないようにすることが重要である。このアクセス権限を確認する認証方法としては、パスワード入力によるものが良く知られるが、アクセスする度にパスワード入力を求める方法は安全である反面ユーザにとっては不便であるため、利便性を向上させたシングルサインオン型の認証方法が利用されるようになって来た。このようなシングルサインオン型の認証方法としては、例えば、Kerberos認証システムで用いられるTTP (Trusted Third-party Protocol) が一般に知られている。

【0003】以下、従来のシングルサインオン型の認証方法について図面を参照しながら説明する。図23は従来のシングルサインオン型の認証方法の概要を示す概念図であり、図24はプロトコルを示すプロトコルシーケンス図である。図23及び図24において、81はユーザインタフェースを持つクライアント手段、82はユーザ認証を行なう認証サーバ手段、83はアクセス権限を判断して利用認可を行なう認可サーバ手段である。

【0004】クライアント手段81と認証サーバ手段82とのユーザ認証手順においては、ユーザインタフェースを介して入力されたユーザ識別子UIDとサーバ識別子SIDとを認証提示情報としてともなった認証要求Authenticate Request801をクライアント手段81が認証サーバ手段82に送り、これに対し認証サーバ手段82がパスワードPWを鍵として暗号化されたセッション鍵SKをとともなった認証応答Authorize Request802を認証チケットTicket803とともに送り返す。

【0005】さらに、クライアント手段81と認可サーバ手段83との利用認可手順においては、クライアント手段

81がセッション鍵SKで暗号化されたユーザ識別子UIDとタイムスタンプTSkとを提示情報としてともなった認可要求Authorize Request804を認証チケットTicket805とともに認可サーバ手段83に送り、これに対し認可サーバ手段83は認証要求Authorize Request804における提示情報と認証チケットTicket805とを検証して、正当と認めれば認可通知Result806を送り返すものである。

【0006】以上のようなプロトコルシーケンスを持つ従来のシングルサインオン型の認証方法において、以下その構成について図25を参照しながら説明する。図25は、従来のシングルサインオン型の認証方法の構成を示す機能ブロック図である。図25においても、81はユーザインタフェースを持つクライアント手段、82はユーザ認証を行なう認証サーバ手段、83はアクセス権限を判断して利用認可を行なう認可サーバ手段である。

【0007】クライアント手段81は、データの送受信を行なう第1の送受信手段311と、ユーザからの入力を得る入力手段811と、受信したセッション鍵を復号するセッション鍵復号手段812と、受信した認証チケットを保持するチケット保持手段314と、認証チケットの保持状態に応じて処理を選択する処理選択手段315と、復号したセッション鍵を秘密裏に記憶する機密記憶手段316と、時刻を計時する証明計時手段813と、セッション鍵を用いて認証済み証明情報を暗号化する証明情報暗号手段814とから構成される。

【0008】また、認証サーバ手段82は、データの送受信を行なう第2の送受信手段321と、時刻を計時する認証計時手段322と、パスワード等のユーザ認証情報が蓄積された認証情報蓄積手段323と、ユーザ認証処理毎に暗号鍵を生成するセッション鍵生成手段821と、パスワードを用いてセッション鍵を暗号化するセッション鍵暗号手段822と、セッション鍵を用いて認証チケットを暗号化するチケット暗号手段823とから構成される。

【0009】また、認可サーバ手段83は、データの送受信を行なう第3の送受信手段331と、時刻を計時する認可計時手段332と、認証チケットを復号するチケット復号手段831と、認証チケットの有効性判定を行なうチケット有効判定手段832と、認証済み証明情報を復号化する証明情報復号手段833と、認証済み証明情報の有効性判定を行なう証明情報有効判定手段834と、認証チケットの内容と認証済み証明情報の内容とを比較照合する認可照合手段835とから構成される。

【0010】以上のように構成された従来のシングルサインオン型の認証方法において、以下その動作について図26を参照しながら説明する。まず、クライアント手段81において、ユーザ自身を示すユーザ識別子UIDと認証サーバ手段82にあらかじめ登録されたユーザ認証用のパスワードPWと利用認可を得る対象のサーバ識別子SIDとがユーザ入力800として入力手段811に入力される(ST3101、ST8101)。入力手段811は、

ユーザ入力800を一時保持するとともにサーバ識別子3101を取出してチケット保持手段314に送る。チケット保持手段314は、サーバ識別子3101に対応する認証チケットデータを検索して(ST3102)、検索結果通知3102を処理選択手段315に送る。処理選択手段315は、検索結果通知3102が無しを示す場合には、ユーザ認証処理起動通知8101を前記入力手段811に送り、有りを示す場合には、利用認可手順起動通知8102を前記チケット保持手段314、機密記憶手段316及び証明情報暗号手段814に送る(ST3103)。

【0011】前記入力手段811は、ユーザ認証起動通知8101が与えられると、一時保持したユーザ入力800から取出した、ユーザ識別子とサーバ識別子との組8103を第1の送受信手段311を介して認証要求Authenticate Request801として認証サーバ手段82に送り(ST8102)、ユーザ識別子8104を証明情報暗号手段814に送り、パスワード8105をセッション鍵復号手段812に送る。

【0012】認証サーバ手段82においては、認証要求Authenticate Request801は第2の送受信手段321で受信され、取出されたユーザ識別子8201が認証情報蓄積手段323及びチケット暗号手段823に送られ、サーバ識別子8202がチケット暗号手段823に送られる(ST8201)。認証情報蓄積手段323は、ユーザ識別子8201に対応するパスワードを検索して(ST8202)、有りの場合にはパスワード8203をセッション鍵暗号手段822に送り、検索結果通知8204をセッション鍵生成手段821及びセッション鍵暗号手段822に送る(ST8203)。セッション鍵生成手段821は、検索結果通知8204が有りを示す場合に、新たにランダムなセッション鍵8205を生成してセッション鍵暗号手段822及びチケット暗号手段823に送る(ST8204)。セッション鍵暗号手段822は、検索結果通知8204が有りを示す場合に、セッション鍵8205をパスワード8203を用いて暗号化した暗号化セッション鍵8206を生成し(ST8205)、これを第2の送受信手段321を介して認証応答Authenticate Response802としてクライアント手段81に送る(ST8207)。認証計時手段322は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ3212をチケット暗号手段823に供給している。チケット暗号手段823は、内部に保持したサーバ識別子8202に対応したサーバ共通鍵を用いて、ユーザ識別子8201とサーバ識別子8202とタイムスタンプ3212とセッション鍵8205とを暗号化した認証チケットデータ8207を生成し(ST8202、ST8206)、これを第2の送受信手段321を介して認証チケットTicket803としてクライアント手段81に送る(ST8207)。

【0013】クライアント手段81においては、認証応答Authenticate Response802は第1の送受信手段311を介して暗号化セッション鍵8106としてセッション鍵復号手段812に送られ、認証チケットTicket803は第1の送受信手段311を介して認証チケットデータ8108として前記チ

チケット保持手段314に送られる(ＳＴ８１０３)。前記チケット保持手段314は認証チケットデータ8108をサーバ識別子3101と対応づけて保持する(ＳＴ３１１２)。セッション鍵復号手段812は、暗号化セッション鍵8106をパスワード8105を用いて復号化する(ＳＴ８１０４)。従って、正しいパスワードが入力された場合にのみ正しいセッション鍵を得ることができる。セッション鍵復号手段812で得られたセッション鍵8107は機密記憶手段316に送られ記憶される。

【００１４】機密記憶手段316は、セッション鍵8107を秘密裏に記憶して所定のアクセスのみ許容するもので(ＳＴ８１０５)、利用認可手順起動通知8102が与えられた場合に、記憶したセッション鍵8109を証明情報暗号手段814に送る。証明計時手段813は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ8110を証明情報暗号手段814に供給している。証明情報暗号手段814は、利用認可手順起動通知8102が与えられると、ユーザ識別子8104とタイムスタンプ8110とをセッション鍵8109を用いて暗号化した認証済み証明情報8111を生成し(ＳＴ８１０６)、これを第１の送受信手段311を介して認可要求Authorize Request804として認可サーバ手段83に送る(ＳＴ８１０７)。前記チケット保持手段314は、利用認可手順起動通知8102が与えられると、サーバ識別子3101に対応する保持した認証チケットデータ8112を、第１の送受信手段311を介して認証チケットTicket805として認可サーバ手段83に送る(ＳＴ８１０７)。

【００１５】認可サーバ手段83においては、認可要求Authorize Request804は第３の送受信手段331を介して認証済み証明情報8308として証明情報復号手段833に送られ、認証チケットTicket805は第３の送受信手段331を介して認証チケットデータ8301としてチケット復号手段831に送られる(ＳＴ８３０１)。チケット復号手段831は、認証チケットデータ8301を内部に保持した自サーバ共通鍵を用いて復号化して、得られたユーザ識別子8302とサーバ識別子8303とタイムスタンプ8304とをチケット有効判定手段832に送り、セッション鍵8305を証明情報復号手段833に送る(ＳＴ８３０２)。認可計時手段332は、現在時刻を計時しており、現在時刻情報8306をチケット有効判定手段832及び証明情報有効判定手段834に供給している。チケット有効判定手段832は、サーバ識別子8303と内部に保持した自サーバ識別子との一致判定を行なうとともに、タイムスタンプ8304と現在時刻情報8306との差が所定の有効期限の範囲内であることをチェックして、いずれも真である場合にユーザ識別子8302をチケットユーザ識別子8307として認可照合手段835に送る(ＳＴ３３０６、ＳＴ３３０７)。証明情報復号手段833は、認証済み証明情報8308をセッション鍵8305を用いて復号化して、得られたユーザ識別子8309とタイムスタンプ8310とを証明情報有効判定手段834に送る(ＳＴ８３０３)。認証済み証明情報はクライアント手段でセ

ッション鍵を用いて暗号化されているので、クライアント手段で正しいセッション鍵が用いられた場合にのみ、ここで正しいユーザ識別子とタイムスタンプとが得られる。証明情報有効判定手段834は、タイムスタンプ8310と現在時刻情報8306との差が所定の時間差の範囲内であることをチェックして、真である場合にユーザ識別子8309を証明ユーザ識別子8311として認可照合手段835に送る(ＳＴ８３０４、ＳＴ８３０５)。認可照合手段835は、チケットユーザ識別子8307と証明ユーザ識別子8311との一致判定を行ない(ＳＴ８３０６)、真であるならば認可通知8312を、第３の送受信手段331を介して認可通知Result806としてクライアント手段81に送り(ＳＴ８３０７、ＳＴ３３１７)、クライアント手段81において受信される(ＳＴ３１１８)。このとき、一致判定が真となった場合、ユーザ識別子とタイムスタンプとが正しく得られており、これはクライアント手段で正しいセッション鍵が用いられたことを示しており、これは正しいパスワードが入力されたことを意味するので、ユーザ認証結果と利用認可結果とが一致することになる。

【００１６】

【発明が解決しようとする課題】しかしながら、上記従来の構成では、多大な計算量を必要とする暗号処理を多用しており、特に利用認可処理のたびにクライアント側で暗号処理を行なう必要があるため、クライアント側が携帯型情報端末やスマートフォンのような計算処理能力の低い装置である場合には、実用的な処理時間で利用認可処理を行なうことが困難であるという課題を有していた。

【００１７】また、上記従来の構成では、１つの認証チケットの使用回数を制限しておらず有効期限を設けているのみであるため、第三者により盗聴された認証チケットの暗号が万一解読されて不正なアクセスが行なわれたとしても、発見されずに終わってしまう可能性が高いという課題も有していた。

【００１８】本発明は、こうした従来の課題を解決するものであり、クライアント側での暗号処理を必要とせず、計算処理能力の低い装置であっても実用的な処理時間で利用認可処理を行なうことができ、認証チケットの使用回数を容易に管理することができる、シングルサインオン型の認証方法及び認証システムを提供することを目的とする。

【００１９】

【課題を解決するための手段】この課題を解決するために、本発明は、第１に、有効回数が n (n は正整数)である認証チケットを保持し、これを示して利用認可を求めるクライアント手段と、これを受けて提示情報を要求し前記認証チケットと照合して利用認可する認可サーバ手段と設け、前記認証チケットは、チケット識別子と照合情報と有効回数と発行日時とサーバ識別子とを含み認証子が付与されたものであり、前記照合情報は、前記認

証チケットの発行者と前記クライアント手段とが共有する秘密情報に所定の不可逆演算を n 回施したものであり、前記認証チケットの使用回数が k (k は n 以下の正整数)であるときの前記提示情報は、前記秘密情報に前記所定の不可逆演算を $n-k$ 回施したものであることを特徴としている。

【0020】これにより、クライアント側での暗号処理を必要とせず、認証チケットの使用回数を容易に管理して二重使用を排除することができる、シングルサインオン型の認証方法及び認証システムが得られる。

【0021】第2に、前記認証サーバ手段は、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求するものであり、前記秘密情報は、前記ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を1回以上施したものであり、前記認証提示情報は、前記秘密情報に前記所定の不可逆演算を n 回施したものであることを特徴としている。

【0022】これにより、上記効果に加えて、ユーザ認証手順においてもクライアント側での暗号処理を必要としないうえ、認証提示情報の演算処理と提示情報の演算処理とが共通化できる、シングルサインオン型の認証方法及び認証システムが得られる。

【0023】第3に、前記認証サーバ手段は、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求するものであり、前記認証提示情報は、前記ユーザ認証情報及び前記乱数との連結に前記所定の不可逆演算を1回以上施したものとクライアント手段が生成した認証用乱数との排他的論理和演算結果であり、前記秘密情報は、前記認証提示情報から逆算される前記認証用乱数であることを特徴としている。

【0024】これにより、上記効果に加えて、認証チケットに含まれる照合情報がユーザ認証情報と無関係となるため認証チケットからユーザ認証情報が推測される可能性すらない、より安全なシングルサインオン型の認証方法及び認証システムが得られる。

【0025】第4に、前記所定の不可逆演算が一方方向性ハッシュ演算であることを特徴としている。

【0026】これにより、上記効果に加えて、クライアント側が計算処理能力の低い装置であっても実用的な処理時間で利用認可処理を行なうことができる、シングルサインオン型の認証方法及び認証システムが得られる。

【0027】第5に、前記認証チケットは発行者識別子を含み、前記認可サーバ手段は、利用認可するとともに前記認証チケットの照合情報と有効回数と発行日時と発行者識別子と認証子とを更新するものであり、前記照合情報は、前記秘密情報に前記所定の不可逆演算を $n-k$ 回施したもので更新され、前記有効回数は、 $n-k$ で更新されることを特徴としている。

【0028】これにより、上記効果に加えて、認証チケットは使用することに更新され、特にタイムスタンプが

更新されるため有効判定における有効期限をより短く設定できるので、第三者による不正使用の可能性をより小さくでき、さらに利用認可の応答時間を短縮できる、シングルサインオン型の認証方法及び認証システムが得られる。

【0029】第6に、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認可サーバ手段を複数備え、前記認証チケットの使用回数を管理する認証チケット管理手段を備えており、前記認証サーバ手段は、前記認証チケットを発行するとともに前記認証チケット管理手段に前記認証チケットの発行登録を指示し、前記認可サーバ手段は、前記認証チケットの提示を受けて前記認証チケット管理手段に前記認証チケットの履歴更新を指示し、前記認証チケット管理手段より拒絶通知を受けた場合には利用認可しないことを特徴としている。

【0030】これにより、上記効果に加えて、認証チケットが更新されないシステムにおいて、認証チケットを複数の認可サーバに対して共通に用いることが可能となるため、より利便性の高い、シングルサインオン型の認証方法及び認証システムが得られる。

【0031】第7に、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認可サーバ手段を複数備え、前記認証サーバ手段は、前記認証チケットを発行するとともに発行履歴を記憶し、前記認可サーバ手段は、前記認証チケットを更新するとともに更新履歴を記憶し、前記認証チケットの提示を受けて前記認証チケットの発行者識別子が示す前記認証サーバ手段または前記認可サーバ手段に前記認証チケットの履歴を照会し、前記認証サーバ手段または前記認可サーバ手段より拒絶通知を受けた場合には利用認可しないことを特徴としている。

【0032】これにより、上記効果に加えて、認証チケットが更新されるシステムにおいて、認証チケットの利用を分散管理できるため1個所の管理リソースをより少なくできる、シングルサインオン型の認証方法及び認証システムが得られる。

【0033】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら説明する。

【0034】(第1の実施の形態)第1の実施形態の認証システムは、図1に示すように、ユーザインタフェースを持つクライアント手段1と、ユーザ認証を行なう認証サーバ手段2と、クライアント手段1のアクセス権限を判断して利用認可を行なう認可サーバ手段3とから成る。クライアント手段1には、例えば汎用コンピュータ、携帯情報端末、スマートフォンなどが使用でき、認証サーバ手段2には、例えば汎用コンピュータ、専用認

証サーバ装置などが使用でき、また、認可サーバ手段3には、汎用コンピュータ、専用認可サーバ装置、専用情報提供装置などが使用できる。

【0035】クライアント手段1と認可サーバ手段3との間には有線または無線通信ネットワークにより接続される。クライアント手段1と認証サーバ手段2との間は必ずしも通信ネットワークで接続されていないが、秘密情報4を共有している必要がある。この秘密情報4としては、例えばパスワード、共通鍵方式暗号鍵、またはそれらから算出される計算値などが用いられる。

【0036】クライアント手段1は、利用認可手順で用いる認証チケット5を保持している。これは認証サーバ手段2がクライアント手段1に対して発行したものであり、認証サーバ手段2は、秘密情報4に不可逆演算 f を n 回（ n は認証チケットの有効回数）行なった結果を照合情報とし、これに認証子を付加して認証チケット5を生成する。認証子は認証チケットの改ざん防止と発行者の証明とを目的として付加されるもので、メッセージ認証コードやデジタル署名などが使用できる。

【0037】クライアント手段1と認可サーバ手段3との利用認可手順においては、クライアント手段1が秘密情報4に不可逆演算 f を $n-k$ 回（ k は認証チケットの利用認可手順での使用回数）行なった結果を提示情報6として用いる。不可逆演算 f が充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この提示情報6は秘密情報4を知らない第三者には計算することができないため、この提示情報6により秘密情報4を知る正当なユーザであることが示される。また、過去にさかのぼるほど提示情報における不可逆演算 f の回数が多く行なわれているため、この提示情報6から次の提示情報を計算することもできないので、暗号化の必要もない。

【0038】クライアント手段1は、この提示情報6を、保持していた認証チケット7とともに認可サーバ手段3に送り、これに対し認可サーバ手段3は、認証チケット7が含む認証子の検証と、提示情報6に不可逆演算 f を k 回行なった結果が認証チケット7が含む照合情報に一致することの確認とを行なって、正当と認めれば認可通知8を送り返す。

【0039】この方法により、クライアント手段1は秘密情報4を認可サーバ手段3を含めた第三者に明かすことなく、 n 回まで認証チケット7を使用して利用認可を得ることができる。

【0040】このように、本実施の形態の認証システムは、有効回数が n （ n は正整数）である認証チケットを保持し、これを示して利用認可を求めるクライアント手段と、これを受けて提示情報を要求し前記認証チケットと照合して利用認可する認可サーバ手段とを具備している。

【0041】前記認証チケットには、照合情報の他に、チケット識別子、有効回数、発行日時、サーバ識別子な

どの情報を含めることができ、これに認証子が付与される。照合情報は、認証チケットの発行者とクライアント手段とが共有する秘密情報に所定の不可逆演算を n 回施した情報である。また、前記提示情報は、認証チケットの使用回数が k （ k は n 以下の正整数）であるとき、前記秘密情報に所定の不可逆演算を $n-k$ 回施した情報である。

【0042】こうした構成により、クライアント側での暗号処理を必要とせず、認証チケットの使用回数を容易に管理して二重使用を排除することができる、シングルサインオン型の認証方法及び認証システムが得られる。

【0043】（第2の実施の形態）第2の実施形態の認証システムでは、クライアント手段が、認証サーバ手段22に対して認証提示情報を示して認証チケットを要求する。

【0044】この認証システムは、図2に示すように、ユーザインタフェースを持つクライアント手段11と、ユーザ認証を行なう認証サーバ手段12と、クライアント手段11のアクセス権限を判断して利用認可を行なう認可サーバ手段3とから成り、クライアント手段11と認証サーバ手段12及び認可サーバ手段3との間には有線または無線通信ネットワークにより接続されている。この認可サーバ手段3は第1の実施形態（図1）と同一であり、また、認証サーバ手段12からクライアント手段11に送り返される認証チケット、クライアント手段11が認可サーバ手段3に送信する提示情報及び認可チケット、さらに認可サーバ手段3からクライアント手段11に送り返される認可通知8についても、第1の実施形態（図1）と同一である。

【0045】この認証システムのクライアント手段11と認証サーバ手段12とは、ユーザインタフェースを介して入力されたパスワード PW と認証サーバ手段12より得た乱数 R との連結に不可逆演算 f を1回行なった結果を秘密情報14として共有する。不可逆演算 f が充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この秘密情報14はパスワード PW を知らない第三者には計算することができない。

【0046】クライアント手段11と認証サーバ手段12とのユーザ認証手順においては、認証サーバ手段12が乱数を生成し、これを示してクライアント手段11に認証提示情報を要求する。クライアント手段11は、パスワード PW と認証サーバ手段12より得た乱数 R との連結に不可逆演算 f を1回行なって秘密情報14を算出し、この秘密情報14にさらに不可逆演算 f を n 回（通算 $n+1$ 回、 n は認証チケットの有効回数）行なった結果を認証提示情報13として認証サーバ手段12に送る。

【0047】これに対し、認証サーバ手段12は、認証提示情報13から秘密情報14が一致していることを確認すると、秘密情報14に不可逆演算 f を n 回行なった結果を照合情報として、これに認証子を付加した認証チケット5

を送り返す。クライアント手段11は、これを利用認可手順で用いるために保持する。認証子は認証チケットの改ざん防止と発行者の証明を目的として付加されるもので、メッセージ認証コードやデジタル署名などが使用できる。

【0048】また、クライアント手段11と認可サーバ手段3との利用認可手順においては、クライアント手段11が秘密情報14に不可逆演算 f を $n-k$ 回（ k は認証チケットの利用認可手順での使用回数）行なった結果を提示情報6として用いる。不可逆演算 f が充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この提示情報6は秘密情報14を知らない第三者には計算することができないため、この提示情報6により秘密情報14を知る正当なユーザであることが示される。また、過去にさかのぼるほど提示情報における不可逆演算 f の回数が多く行なわれているため、この提示情報6から次の提示情報を計算することもできないので、暗号化の必要もない。

【0049】クライアント手段11は、この提示情報6を、保持していた認証チケット7とともに認可サーバ手段3に送り、これに対し認可サーバ手段3は認証チケット7が含む認証子の検証と、提示情報6に不可逆演算 f を k 回行なった結果が認証チケット7が含む照合情報に一致することの確認とを行なって、正当と認めれば認可通知8を送り返す。

【0050】この方法により、クライアント手段11は秘密情報14やパスワードPWを認可サーバ手段3を含めた第三者に明かすことなく、 n 回まで認証チケット7を使用して利用認可を得ることができる。

【0051】このように、本実施の形態の認証システムでは、認証サーバ手段が、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求する。このときの秘密情報として、ユーザ認証情報と乱数との連結に所定の不可逆演算を1回以上施したものを使用し、認証提示情報として、この秘密情報に所定の不可逆演算を n 回施したものが提示される。

【0052】こうした構成により、第1の実施形態の効果に加えて、ユーザ認証手順においてもクライアント側での暗号処理が不要であり、また、認証提示情報の演算処理と提示情報の演算処理とが共通化できる、シングルサインオン型の認証方法及び認証システムが得られる。

【0053】（第3の実施の形態）第3の実施形態の認証システムでは、図3に示すように、クライアント手段21によって生成された認証用乱数が秘密情報24としてクライアント手段21と認証サーバ手段22との間で共有される。

【0054】このシステムでは、ユーザ認証手順において、認証サーバ手段22が乱数を生成し、これを示してクライアント手段21に認証提示情報を要求する。クライアント手段21は、パスワードPWと認証サーバ手段22より

得た乱数Rとの連結に不可逆演算 f を1回行なった結果とクライアント手段21が秘密裏に生成した秘密情報24との排他的論理和結果を認証提示情報23として認証サーバ手段22に送る。図3において、記号「@」は排他的論理和（EXOR）演算を示している。

【0055】これに対し、認証サーバ手段22は、認証提示情報23とパスワードPWと乱数Rとから逆算して秘密情報25を求める。そして、この秘密情報25に不可逆演算 f を n 回行ない、その演算結果を照合情報とし、これに認証子を付加した認証チケット5をクライアント手段21に送り返す。クライアント手段21は、これを利用認可手順で用いるために保持する。

【0056】なお、もしユーザが不正な第三者で認証提示情報23が適当に作られたものだとなれば、クライアント手段21で認証チケット5を入手することができても、サーバが認証提示情報23からパスワードPWと乱数Rとを用いて逆算した秘密情報25はクライアント手段21には分からない。そのため、後続の利用認可手順においてその不正なアクセスを排除することができる。

【0057】クライアント手段21と認可サーバ手段3との利用認可手順においては、クライアント手段21が秘密情報24に不可逆演算 f を $n-k$ 回（ k は認証チケットの利用認可手順での使用回数）行なった結果を提示情報6として用いる。不可逆演算 f が充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この提示情報6は秘密情報24を知らない第三者には計算することができないため、この提示情報6により秘密情報24を知る正当なユーザであることが示される。また、過去にさかのぼるほど提示情報における不可逆演算 f の回数が多く行なわれているため、この提示情報6から次の提示情報を計算することもできないので、暗号化の必要もない。

【0058】クライアント手段21は、この提示情報6を、保持していた認証チケット7とともに認可サーバ手段3に送り、これに対し認可サーバ手段3は認証チケット7が含む認証子の検証と、提示情報6に不可逆演算 f を k 回行なった結果が認証チケット7が含む照合情報に一致することの確認とを行なって、正当と認めれば認可通知8を送り返す。

【0059】この方法により、クライアント手段21は、秘密情報24やパスワードPWを認可サーバ手段3を含めた第三者に明かすことなく、 n 回まで認証チケット7を使用して利用認可を得ることができる。

【0060】このように、本実施の形態の認証システムでは、認証サーバ手段は、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求する。認証提示情報は、ユーザ認証情報及び前記乱数との連結に所定の不可逆演算を1回以上施したものと、クライアント手段が生成した認証用乱数（秘密情報）との排他的論理和演算結果であり、この秘密情報は、認証サーバ手段により認証提示情報から逆算され

る。

【0061】こうした構成により、認証チケットが含む照合情報がユーザ認証情報と無関係となる。そのため認証チケットからユーザ認証情報が推測される可能性すらないより安全な、シングルサインオン型の認証方法及び認証システムが得られる。

【0062】（第4の実施の形態）第4の実施形態では、第2の実施形態の認証システムにおける具体的な通信手順とそれを実行する各手段のブロック構成について説明する。

【0063】図4は、このシステムでのプロトコルを示すプロトコルシーケンス図である。図4において、31はユーザインタフェースを持つクライアント手段、32はユーザ認証を行なう認証サーバ手段、33はアクセス権限を判断して利用認可を行なう認可サーバ手段を示し、記号「S(K|~)」は鍵Kを用いた認証子添付関数を示している。

【0064】クライアント手段31と認証サーバ手段32とのユーザ認証手順においては、まず、クライアント手段31が、ユーザインタフェースを介して入力されたユーザ識別子UIDとサーバ識別子SIDとをともなった認証要求Authenticate Request301を認証サーバ手段32に送る。この時、認証要求Authenticate Request301が認証チケットの有効回数nをともなうものとしてもよい。そうでない場合には、認証サーバが固定的に有効回数nを定めるものとすればよい。

【0065】これに対して、認証サーバ手段32は、毎回異なるように生成された乱数R0をともなった認証チャレンジChallenge302を送り返す。これを受けたクライアント手段31は、ユーザインタフェースを介して入力されたパスワードPWと乱数R0との連結に対してn+1段のハッシュ演算Hを施した結果をともなった認証チャレンジ応答Response303を送り返し、これに対し認証サーバ手段32は、チャレンジ応答Response303におけるn+1段ハッシュ演算結果と自ら行なったn+1段ハッシュ演算結果とを比較検証して一致すれば正当と認め、新たに生成したチケット識別子TIDとn+1段ハッシュ演算結果とタイムスタンプTS0とサーバ識別子SIDと認証サーバ32自身を示す発行者識別子IIDとをともない認証子が付加された認証チケットTicket304を送り返す。クライアント手段31は、これを利用認可手順で用いるために保持する。

【0066】また、クライアント手段31と認可サーバ手段33との利用認可手順においては、クライアント手段31が認可要求Authorize Request及び認証チケットTicket305を認可サーバ手段33に送る。この時、認可要求Authorize Requestがユーザ識別子UIDをともなうものとしてもよい。これに対して、認可サーバ手段33は、この認証チケットの使用回数に基づく値kをともなった認可チャレンジChallenge306を送り返す。これを受けたクライ

アント手段31は、パスワードPWと乱数R0との連結に対してn-k+1段のハッシュ演算Hを施した結果をともなった認可チャレンジ応答Response307を送り返す。

【0067】このハッシュ演算Hが充分安全な方向性と結果の長さ及びランダム性を持っている限り、このハッシュ演算結果はパスワードPW及び乱数R0を知らない第三者には計算することができないため、このハッシュ演算結果によりパスワードPWを知る正当なユーザであることが示される。また、過去にさかのぼるほどハッシュ演算Hの段数が多く行なわれているため、このハッシュ演算結果から次のハッシュ演算結果を計算することもできないので、暗号化の必要もない。このようなハッシュ演算Hとしては、例えばMD5やSHAなどのアルゴリズムを使用することができる。

【0068】これに対して、認可サーバ手段32は、認可チャレンジ応答Response307におけるn-k+1段ハッシュ演算結果にさらにk段のハッシュ演算を施した結果と認証チケットTicketにおけるn+1段ハッシュ演算結果とを比較検証し、一致すれば正当と認めて認可通知Result308を送り返す。この時、認可通知308が利用認可によりアクセスが許可された情報Infoを同時にともなうものとしてもよい。

【0069】以上のようなプロトコルシーケンスにより、クライアント手段31はパスワードPWを認可サーバ手段33を含めた第三者に明かすことなく、n回まで認証チケット304を使用して利用認可を得ることができる。

【0070】このようなプロトコルシーケンスを持つ認証システムの構成について図5の機能ブロック図を参照しながら説明する。

【0071】図5において、31はユーザインタフェースを持つクライアント手段、32はユーザ認証を行なう認証サーバ手段、33はアクセス権限を判断して利用認可を行なう認可サーバ手段である。

【0072】クライアント手段31は、データの送受信を行なう第1の送受信手段311と、ユーザからの入力を得る入力手段312と、2つの入力を連結してハッシュ演算Hを行なうハッシュ手段313と、受信した認証チケットを保持するチケット保持手段314と、認証チケットの保持状態に応じて処理を選択する処理選択手段315と、ハッシュ演算結果を秘密裏に記憶する機密記憶手段316と、与えられた段数または与えられた2つの数値の差の段数のハッシュ演算を行なう多段ハッシュ手段317とを備えている。

【0073】第1の送受信手段311は、通信ネットワークの種類に応じて例えばLANカード等のLANインタフェース装置、ターミナルアダプタ等のISDNインタフェース装置、モデム等の電話インタフェース装置、携帯データ通信カードやPIAFSカード等の無線インタフェース装置、IrDAモジュール等の赤外線インタフェース装置などで構成され、通信相手に応じてこれらの

いくつかを使い分ける構成としてもよい。入力手段312は、例えばキーボード、テンキー等の文字入力装置、マウス、トラックボール、ペンタブレット等のポインティングデバイスや選択ボタンやダイヤルと表示画面との組合せ、あるいはタッチパネルなどで構成される。ハッシュ手段313は、例えば論理回路とハッシュ演算Hのアルゴリズムを組み込んだ演算回路とを組み合わせて構成される。チケット保持手段314は、例えばメモリ回路が使用される。処理選択手段315は、例えば論理回路が使用できる。機密記憶手段316は、例えばICカードのような耐タンパ性を持ったメモリデバイスによって構成される。多段ハッシュ手段317は、例えばハッシュ演算Hのアルゴリズムを組み込んだ演算回路に出力をフィードバックする結線や段数をカウントするカウンタや数値の差を求める演算回路などを追加して構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【0074】また、認証サーバ手段32は、データの送受信を行なう第2の送受信手段321と、現在時刻を計時する認証計時手段322と、パスワード等のユーザ認証情報を蓄積する認証情報蓄積手段323と、ユーザ認証処理毎に乱数を生成する乱数生成手段324と、与えられたよりも1多い段数のハッシュ演算Hを行なう第2の多段ハッシュ手段325と、2つの多段ハッシュ値を比較照合する認証照合手段326と、認証チケット発行毎にユニークなチケット識別子を生成するチケット識別子生成手段327と、認証チケットに対する認証子を生成して付加する認証子付加手段328とを備えている。

【0075】第2の送受信手段321は、通信ネットワークの種類に応じて例えばLANカード等のLANインタフェース装置、ターミナルアダプタ等のISDNインタフェース装置、モデム等の電話インタフェース装置、携帯データ通信カードやPIAFSカード等の無線インタフェース装置、IrDAモジュール等の赤外線インタフェース装置などで構成される。認証計時手段322は、例えばタイマカウンタが使用される。認証情報蓄積手段323は、大容量のメモリデバイスで構成され、耐タンパ性を持ったメモリデバイスであればなお良い。乱数生成手段324は、例えば乱数生成アルゴリズムを組み込んだ演算回路、あるいは電磁的ノイズをデータ化する変換装置などで構成される。第2の多段ハッシュ手段325は、例えばハッシュ演算Hのアルゴリズムを組み込んだ演算回路に出力をフィードバックする結線や段数をカウントするカウンタなどを追加して構成される。認証照合手段326は、例えば比較回路で構成される。チケット識別子生成手段327は、例えば充分なビット長を持ったカウンタ

回路で構成される。認証子付加手段328は、認証子生成アルゴリズムを組み込んだ演算回路及びメモリ回路で構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【0076】また、認可サーバ手段33は、データの送受信を行なう第3の送受信手段331と、現在時刻を計時する認可計時手段332と、認証チケットに付加された認証子を検証する認証子検証手段333と、認証チケットの有効性判定を行なうチケット有効判定手段334と、認証チケットのチケット識別子と有効回数と残り利用可能回数を管理するチケット利用管理手段335と、与えられた段数のハッシュ演算Hを行なう第3の多段ハッシュ手段336と、2つの多段ハッシュ値を比較照合する認可照合手段337とを備えている。

【0077】第3の送受信手段331は、通信ネットワークの種類に応じて例えばLANカード等のLANインタフェース装置、ターミナルアダプタ等のISDNインタフェース装置、モデム等の電話インタフェース装置、携帯データ通信カードやPIAFSカード等の無線インタフェース装置、IrDAモジュール等の赤外線インタフェース装置などで構成される。認可計時手段332は、例えばタイマカウンタが使用される。認証子検証手段333は、認証子検証アルゴリズムを組み込んだ演算回路及びメモリ回路で構成される。チケット有効判定手段334は、例えば比較回路の組合せにより構成される。チケット利用管理手段335は、利用回数を計算する演算回路と大容量のメモリデバイスとの組合せにより構成される。第3の多段ハッシュ手段336は、例えば第2の多段ハッシュ手段325と同様の演算回路でカウンタのプリセット値を改めもので構成される。認可照合手段337は、例えば比較回路で構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【0078】以上のように構成された認証方法及び認証システムにおいて、以下その動作について図6を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数nをとともう場合について説明する。

【0079】まず、クライアント手段31において、ユーザ自身を示すユーザ識別子UIDと認証サーバ手段32にあらかじめ登録されたユーザ認証用のパスワードPWと利用認可を得る対象のサーバ識別子SIDと認証チケットの有効回数nとがユーザ入力300として入力手段312に

入力される（ST3101、ST3104）。入力手段312は、ユーザ入力300を一時保持するとともにサーバ識別子3101を取出してチケット保持手段314に送る。チケット保持手段314は、サーバ識別子3101に対応する認証チケットデータを検索して（ST3102）、検索結果通知3102を処理選択手段315に送る。処理選択手段315は、検索結果通知3102が無しを示す場合には、ユーザ認証処理起動通知3103を前記入力手段312及び多段ハッシュ手段317に送り、有りを示す場合には（ST3103）、利用認可手順起動通知3104を前記チケット保持手段314と機密記憶手段316と多段ハッシュ手段317とに送る。

【0080】前記入力手段312は、ユーザ認証起動通知3103が与えられると、一時保持したユーザ入力300から取出した、ユーザ識別子とサーバ識別子と有効回数の組3105を第1の送受信手段311を介して認証要求Authenticate Request301として認証サーバ手段32に送り（ST3105）、有効回数3106を多段ハッシュ手段317に送り、パスワード3107をハッシュ手段313に送る。

【0081】認証サーバ手段32においては、認証要求Authenticate Request301は第2の送受信手段321で受信され、取出されたユーザ識別子3201が認証情報蓄積手段323に送られ、有効回数3202が第2の多段ハッシュ手段325及び認証子付加手段328に送られ、サーバ識別子3203が認証子付加手段328に送られる（ST3201）。認証情報蓄積手段323は、ユーザ識別子3201に対応するパスワードを検索して（ST3202）、有りの場合には（ST3203）、パスワード3204を第2の多段ハッシュ手段325に送り、検索結果通知3205を乱数生成手段324及び第2の多段ハッシュ手段325に送る。

【0082】乱数生成手段324は、検索結果通知3205が有りを示す場合に、データ攪乱用のチャレンジ乱数3206を新たにランダムに生成して第2の多段ハッシュ手段325に送るとともに、第2の送受信手段321を介して認証チャレンジChallenge302としてクライアント手段31に送る（ST3204）。第2の多段ハッシュ手段325は、検索結果通知3205が有りを示す場合に、パスワード3204とチャレンジ乱数3206との連結に対し有効回数3202より1多い段数のハッシュ演算Hを行なって、結果の多段ハッシュ値3207を認証照合手段326に送る（ST3205）。

【0083】これに対してクライアント手段31においては、認証チャレンジChallenge302は第1の送受信手段311で受信され、チャレンジ乱数3108が取り出されてハッシュ手段313に送られる（ST3106）。ハッシュ手段313はパスワード3107とチャレンジ乱数3108との連結に対するハッシュ演算Hを行なって（ST3107）、結果のハッシュ値3109を機密記憶手段316及び多段ハッシュ手段317に送る。機密記憶手段316はハッシュ値3109を秘密裏に記憶して所定のアクセスのみ、すなわちユー

ザ認証手順における追加更新及び利用認可手順における参照のみ許容する（ST3108）。多段ハッシュ手段317は、ユーザ認証手順起動通知3103が与えられている時、ハッシュ値3109に有効回数3106に相当する段数のハッシュ演算Hを行なって（ST3109）、結果の多段ハッシュ値3114を、第1の送受信手段311を介して認証チャレンジ応答Response303として認証サーバ手段32に送る（ST3110）。

【0084】これに対して認証サーバ手段32においては、認証チャレンジ応答Response303は第2の送受信手段321で受信され、多段ハッシュ値3208が取出されて認証照合手段326に送られる（ST3206）。認証照合手段326は、多段ハッシュ値3207と多段ハッシュ値3208との一致判定を行ない（ST3207）、照合結果3209をチケット識別子生成手段327に送るとともに多段ハッシュ値3208をそのまま多段ハッシュ値3210として認証子付加手段328に送る。チケット識別子生成手段327は、照合結果327が一致を示す場合に、有効なチケット識別子3212を生成して認証子付加手段328に送る（ST3208）。

【0085】認証計時手段322は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ3211を認証子付加手段328に供給している。認証子付加手段328は、チケット識別子3212と多段ハッシュ値3210と有効回数3202とタイムスタンプ3211とサーバ識別子3203と認証サーバ32自身を示す発行者識別子とを連結し、これに対して認証子を生成して付加して認証チケットデータ3213とし（ST3209）、第2の送受信手段321を介して認証チケットTicket304としてクライアント手段31に送る（ST3210）。

【0086】これに対してクライアント手段31においては、認証チケットTicket304は第1の送受信手段311で受信され、認証チケットデータ3110が取出されて前記チケット保持手段314に送られる（ST3111）。前記チケット保持手段314は認証チケットデータ3110をサーバ識別子3101と対応づけて保持し（ST3112）、利用認可手順起動通知3104が与えられた場合に、認証チケットデータ3111を第1の送受信手段311を介して認証チケットTicket305として認可要求Authorize Requestとともに認可サーバ手段33に送る（ST3113）とともに、認証チケットデータから有効回数3112を取出して多段ハッシュ手段317に送る。

【0087】これに対して認可サーバ手段33においては、認証チケットTicket305をともなった認可要求Authorize Requestは第3の送受信手段331で受信され、認証チケットデータ3301が取出されて認証子検証手段333に送られる（ST3301）。認証子検証手段333は、認証チケットデータ3301の認証子と認証子以外のデータ部との整合性を検証して検証結果3304をチケット有効判定手段334に送るとともに（ST3304）、データ部が

らタイムスタンプ3302とサーバ識別子3303とを取出してチケット有効判定手段334に、チケット識別子3305と多段ハッシュ値3306と有効回数3307と発行者識別子3308とを取出してチケット利用管理手段335に、それぞれ送る。

【0088】認可計時手段332は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ3309をチケット有効判定手段334に供給している。チケット有効判定手段334は、検証結果3304が誤りなしを示す場合に（ST3305）、サーバ識別子3303と内部に保持した自サーバ識別子との一致判定を行なうとともに（ST3302、ST3303）、タイムスタンプ3302と現在時刻に基づくタイムスタンプ3309との差が所定の有効期限の範囲内であることをチェックして（ST3306、ST3307）、いずれも真である場合にチケット有効通知3310をチケット利用管理手段335に送る。この有効期限は、短く設定するとセキュリティは向上するがユーザ利便性は低下し、長く設定するとユーザ利便性は向上するがセキュリティは低下するため、これらのバランスを勘案して定めるべきである。例えば厳重なセキュリティまでは要求されていない業務用システムに適用するならば1日の勤務時間をカバーできる8時間なり12時間なりにすればよい。ただし、最短でもクライアント～サーバ間の通信時間及び各計時手段の間の時刻誤差をカバーできる必要がある。

【0089】このとき、チケット利用管理手段335はチケットリストを管理しており、チケット有効通知3310が与えられた場合に、チケット識別子3305を用いてチケットリスト中を検索して既に登録されているかを調べる（ST3308）。該当するものが無ければチケット識別子3305と有効回数3307と残り利用可能回数とを示す値としての有効回数3307の組をチケットリストに追加し記憶する（ST3309、ST3310）。この時、多段ハッシュ値3306と発行者識別子3308をあわせて記憶してもよい。この追加した組、あるいは検索で該当するものがあった場合は当該の組に対し、チケット利用管理手段335は残り利用可能回数を1減じ、有効回数と残り利用可能回数との差が示す利用回数3311を求め（ST3311）、これを第3の送受信手段331を介して認可チャレンジChallenge306としてクライアント手段31に送るとともに（ST3312）、第3の多段ハッシュ手段336にも送る。また、多段ハッシュ値3306をそのまま多段ハッシュ値3312として認可照合手段337に送る。

【0090】これに対してクライアント手段31においては、認可チャレンジChallenge306は第1の送受信手段311で受信され、利用回数3115が取出されて多段ハッシュ手段317に送られる（ST3114）。多段ハッシュ手段317は、利用認可手順起動通知3104が与えられている場合に、前記機密記憶手段316よりハッシュ値3113を得て（ST3115）、ハッシュ値3113に有効回数3112と

利用回数3115との差に相当する段数のハッシュ演算Hを行なって（ST3116）、結果の多段ハッシュ値3116を、第1の送受信手段311を介して認可チャレンジ応答Response307として認可サーバ手段33に送る（ST3117）。

【0091】ハッシュ演算Hが充分安全な方向性と結果の長さ及びランダム性を持っている限り、この多段ハッシュ値3116はパスワードPW及び乱数ROを知らない第三者には計算することができないため、この多段ハッシュ値3116によりパスワードPWを知る正当なユーザであることが示される。また、過去にさかのぼるほど多段ハッシュ値におけるハッシュ演算Hの段数が多く行なわれているため、この多段ハッシュ値3116から次の多段ハッシュ値を計算することもできないので、暗号化の必要もない。なお、ハッシュ演算は一般に暗号演算よりも100倍以上高速であるとされ、適切な段数であれば暗号を用いた場合よりも高速に処理が行なえる。

【0092】これに対して認可サーバ手段33においては、認可チャレンジ応答Response307は第3の受信手段331で受信され、多段ハッシュ値3313が取出されて第3の多段ハッシュ手段336に送られる（ST3313）。第3の多段ハッシュ手段336は、多段ハッシュ値3313に利用回数3311に相当する段数のハッシュ演算Hを行なって、結果の二次多段ハッシュ値3314を認可照合手段337に送る（ST3314）。認可照合手段337は、多段ハッシュ値3312と二次多段ハッシュ値3314との一致判定を行ない（ST3315、ST3316）、真であるならば認可通知3315を、第3の送受信手段331を介して認可通知Result308としてクライアント手段31に送り（ST3317）、クライアント手段31において受信される（ST3118）。この方法により、クライアント手段31はパスワードPWを認可サーバ手段33を含めた第三者に明かすことなく、n回まで認証チケット305を使用して利用認可を得ることができる。

【0093】なお、以上の説明ではクライアント手段31において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【0094】次に、図5に示した第4の実施形態の認証システムにおいて、認証子としてメッセージ認証コードを用いた場合の認証子付加手段328及び認証子検証手段333の詳細な構成例及び動作について、図7及び図8を参照して説明する。

【0095】認証子付加手段328は、図7に示すように、認証サーバ自身を示す識別子が記憶された自識別子記憶手段328Aと、データを連結するデータ連結手段328B

と、ハッシュ演算 h を行なう連結データハッシュ手段328Cと、認証サーバ手段31と認可サーバ手段32とが共通の秘密として持つサーバ共通鍵を記憶するサーバ共通鍵記憶手段328Dと、共通鍵方式の暗号処理を行なう共通鍵方式暗号手段328Eと、認証子をデータに連結する認証子連結手段328Fとを具備している。

【0096】この自識別子記憶手段328Aは、例えばメモリで構成される。データ連結手段328Bは、例えば論理回路で構成される。連結データハッシュ手段328Cは、例えばハッシュ演算 h のアルゴリズムを組み込んだ演算回路で構成される。ここでハッシュ演算 h は、ハッシュ演算 H と同じであっても異なっても良い。サーバ共通鍵記憶手段328Dは、例えばメモリで構成され、耐タンパ性を持ったメモリデバイスであればなお良い。共通鍵方式暗号手段328Eは、例えば暗号アルゴリズムを組み込んだ演算回路または暗号処理専用プロセッサで構成される。ここで暗号アルゴリズムとしては、例えばDESやトリプルDESなどが使用できる。認証子連結手段328Fは、例えば論理回路で構成される。

【0097】また、認証子検証手段333は、図8に示すように、認証子をデータから分離する認証子分離手段333Aと、ハッシュ演算 h を行なう第2の連結データハッシュ手段333Bと、認証サーバ手段31と認可サーバ手段32とが共通の秘密として持つサーバ共通鍵を記憶する第2のサーバ共通鍵記憶手段333Cと、共通鍵方式の暗号処理を行なう第2の共通鍵方式暗号手段333Dと、データ部を分割分離するデータ分離手段333Eと、発行者識別子を照合する発行者識別子照合手段333Fと、メッセージ認証コードを比較検証する比較手段333Gと具備している。

【0098】この認証子分離手段333Aは、例えば論理回路で構成される。第2の連結データハッシュ手段333B、第2のサーバ共通鍵記憶手段333C及び第2の共通鍵方式暗号手段333Dは、それぞれ図7における328C、328D、328Eと同じように構成される。データ分離手段333Eは、例えば論理回路で構成される。発行者識別子照合手段333Fは、例えばメモリ回路及び比較回路で構成される。比較手段333Gは、例えば比較回路の組合せにより構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【0099】以上のように構成された認証子付加手段328及び認証子検証手段333の動作について説明する。認証子付加手段328では、まず、自識別子記憶手段328Aからデータ連結手段328Bに認証サーバ自身を示す識別子が発行者識別子328aとして供給されている。データ連結手段328Bは、第2の送受信手段321より得た有効回数3202及びサーバ識別子3203と、認証照合手段326より得た多段

ハッシュ値3210と、認証計時手段322より得たタイムスタンプ3211と、チケット識別子生成手段327より得たチケット識別子3212と、自識別子記憶手段328Aより得た発行者識別子328aとを定められた順序で並べて連結し、データ部328bとして連結データハッシュ手段328C及び認証子連結手段328Fに送る。

【0100】連結データハッシュ手段328Cは、データ部328bに対するハッシュ演算 h を行なって、結果のハッシュ値328cを共通鍵方式暗号手段328Eに送る。共通鍵方式暗号手段328Eは、サーバ共通鍵記憶手段328Dからサーバ共通鍵328dを得て、これを暗号鍵に用いてハッシュ値328cを暗号化して、メッセージ認証コード328eとして認証子連結手段328Fに送る。認証子連結手段328Fは、データ部328bにメッセージ認証コード328eを連結して、認証チケットデータ3213を出力する。

【0101】また、認証子検証手段333では、まず、認証チケットデータ3301が認証子分離手段333Aに入力され、メッセージ認証コード333aとデータ部333bとに分離され、メッセージ認証コード333aは比較手段333Gに、データ部333bは第2の連結データハッシュ手段333B及びデータ分離手段333Eにそれぞれ送られる。第2の連結データハッシュ手段333Bは、データ部333bに対するハッシュ演算 h を行なって、結果のハッシュ値333cを第2の共通鍵方式暗号手段333Dに送る。第2の共通鍵方式暗号手段333Dは、第2のサーバ共通鍵記憶手段333Cからサーバ共通鍵333dを得て、これを暗号鍵に用いてハッシュ値333cを暗号化して、比較用メッセージ認証コード333eとして比較手段333Gに送る。データ分離手段333Eは、データ部333bをタイムスタンプ3302とサーバ識別子3303とチケット識別子3305と多段ハッシュ値3306と有効回数3307と発行者識別子3308とに分離して出力するとともに、発行者識別子3308については発行者識別子照合手段333Fにも送る。発行者識別子照合手段333Fは、発行者識別子3308が認証サーバ32の識別子かどうかを照合し、照合結果333fを比較手段333Gに送る。比較手段333Gは、照合結果333fが一致を示すか、メッセージ認証コード333aと比較用メッセージ認証コード333eとが一致するかをもとに検証結果3304を出力する。検証結果3304が誤りなしを示すのは、いずれも一致した場合である。

【0102】次に、図5の第4の実施形態の認証システムにおいて、認証子としてデジタル署名を用いた場合の認証子付加手段328及び認証子検証手段333の構成及び動作について、図9及び図10を参照して説明する。図9において図7と異なるのは、サーバ共通鍵記憶手段328D及び共通鍵方式暗号手段328Eの代わりに、認証サーバ32自身の公開鍵方式暗号秘密鍵を記憶する自秘密鍵記憶手段328G及び公開鍵方式の暗号処理を行なう公開鍵方式暗号手段328Hを設けた点にある。自秘密鍵記憶手段328Gとしては、例えばメモリが使用でき、耐タンパ性を持ったメモリデバイスであればなお良い。公開鍵方式暗号手段

328Hとしては、例えば暗号アルゴリズムを組み込んだ演算回路または暗号処理専用プロセッサが使用できる。ここで暗号アルゴリズムとしては、例えばRSAや楕円曲線暗号などが使用できる。

【0103】また、図10において図8と異なるのは、第2のサーバ共通鍵記憶手段333C、第2の共通鍵方式暗号手段333D及び発行者識別子照合手段333Fの代わりに、認証サーバ手段31の公開鍵をサーバ識別子と対応づけて1つ以上蓄積するサーバ公開鍵蓄積手段333H及び公開鍵方式暗号の復号処理を行なう公開鍵方式復号手段333Jを設け、これらの間の結線を改めた点にある。サーバ公開鍵蓄積手段333Hは、認証サーバ手段32のみならず認可サーバ手段33の公開鍵をも蓄積するものとしてもよい。サーバ公開鍵蓄積手段333Hとしては、例えばメモリ回路が使用でき、大容量のメモリデバイスであればなお良い。公開鍵方式復号手段333Jとしては、例えば復号アルゴリズムを組み込んだ演算回路または暗号処理専用プロセッサが使用できる。ここで復号アルゴリズムとしては、公開鍵方式暗号手段328Hにおける暗号アルゴリズムに対応する復号アルゴリズムを用いることは言うまでもない。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【0104】以上のように構成された認証子付加手段328及び認証子検証手段333の動作について説明する。認証子付加手段328では、自識別子記憶手段328A、データ連結手段328B、連結データハッシュ手段328Cの動作は図7の場合と同様であり、データ部328bが認証子連結手段328Fに、ハッシュ値328cが公開鍵方式暗号手段328Hに、それぞれ供給される。公開鍵方式暗号手段328Hは、自秘密鍵記憶手段328Gから自秘密鍵328fを得て、これを暗号鍵に用いてハッシュ値328cを暗号化して、デジタル署名328gとして認証子連結手段328Fに送る。認証子連結手段328Fは、データ部328bにデジタル署名328gを連結して、認証チケットデータ3213を出力する。

【0105】また、認証子検証手段333では、まず、認証チケットデータ3301が認証子分離手段333Aに入力され、デジタル署名333gとデータ部333bとに分離され、デジタル署名333gは公開鍵方式復号手段333Jに、データ部333bは第2の連結データハッシュ手段333B及びデータ分離手段333Eにそれぞれ送られる。第2の連結データハッシュ手段333Bは、データ部333bに対するハッシュ演算1を行なって、結果のハッシュ値333hを比較手段333Gに送る。データ分離手段333Eは、データ部333bをタイムスタンプ3302とサーバ識別子3303とチケット識別子3305と多段ハッシュ値3306と有効回数3307と発行者識別子3308とに分離して出力するとともに、発行者識別子3308につい

てはサーバ公開鍵蓄積手段333Hにも送る。サーバ公開鍵蓄積手段333Hは、発行者識別子3308が既知の認証サーバ31（または認可サーバ32）の識別子かどうか検索照合し、照合結果333iを比較手段333Gに送るとともに、発行者識別子3308に対応するサーバ公開鍵333jを公開鍵方式復号手段333Jに送る。

【0106】公開鍵方式復号手段333Jは、サーバ公開鍵333jを復号鍵に用いてデジタル署名333gを復号化して、比較用ハッシュ値333kとして比較手段333Gに送る。比較手段333Gは、照合結果333iが一致を示すか、ハッシュ値333hと比較用ハッシュ値333kとが一致するかをもとに検証結果3304を出力する。検証結果3304が誤りなしを示すのは、いずれも一致した場合である。

【0107】このように、認証システムがこの実施形態の構成を採ることにより、クライアント側が計算処理能力の低い装置であっても、実用的な処理時間で利用認可処理を行なうことが可能になる。

【0108】（第5の実施の形態）第5の実施形態では、第3の実施形態の認証システムにおける具体的な通信手順とそれを実行する各手段のブロック構成について説明する。

【0109】図11は第5の実施形態における認証システムのプロトコルを示すプロトコルシーケンス図である。図11において図4と異なるのは、ユーザインタフェースを持つクライアント手段41とユーザ認証を行なう認証サーバ手段42とであって、認可サーバ手段33は変わりが無い。また、認証チャレンジ応答Response401がユーザインタフェースを介して入力されたパスワードPWと乱数R0との連結に対して1段のハッシュ演算Hを施した結果とクライアント手段41が秘密裏に生成した認証用乱数S0との排他的論理和結果（記号「@」は排他的論理和演算を示す）をとまなう点、認証チケットTicket402、403がともなうハッシュ演算結果が認証用乱数S0に対するn段のハッシュ演算結果である点、認可チャレンジ応答Response404がともなうハッシュ演算結果が認証用乱数S0に対するn-k段のハッシュ演算である点が異なる。

【0110】以上のようなプロトコルシーケンスにより、クライアント手段41はパスワードPWを認可サーバ手段33を含めた第三者に明かすことなく、n回まで認証チケット402を使用して利用認可を得ることができ、認証チケット402がパスワードPWに無関係の内容であるため、不正な第三者によるパスワードPWを盗むための攻撃対象にすならず、より安全性が高い。

【0111】このようなプロトコルシーケンスを持つ認証システムの構成について図12の機能ブロック図を参照しながら説明する。

【0112】図12においても図5と異なるのは、ユーザインタフェースを持つクライアント手段41及びユーザ認証を行なう認証サーバ手段42であって、認可サーバ手

段33は変わらない。また、クライアント手段41において図5のクライアント手段31と異なるのは、ユーザ認証処理毎に乱数を生成する認証用乱数生成手段411、及びビット毎の排他的論理和演算を行なう第1の排他的論理和手段412を設け、一部の結線を改めた点にある。また、認証サーバ手段42において図5の認証サーバ手段32と異なるのは、第2の多段ハッシュ手段325、認証照合手段326の代わりに、ハッシュ演算Hを行なう第2のハッシュ手段421、ビット毎の排他的論理和演算を行なう第2の排他的論理和手段422、与えられた段数のハッシュ演算Hを行なう第2の多段ハッシュ手段423を設け、一部の結線を改めた点にある。認証用乱数生成手段411としては、例えば乱数生成アルゴリズムを組み込んだ演算回路、あるいは電磁的ノイズをデータ化する変換装置などが使用できる。第1、第2の排他的論理和手段412、422としては、例えば論理回路が使用できる。第2のハッシュ手段421としては、例えばハッシュ演算Hのアルゴリズムを組み込んだ演算回路が使用できる。第2の多段ハッシュ手段423としては、例えば421と同様の演算回路に出力をフィードバックする結線や段数をカウントするカウンタなどを追加して構成できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読み取り装置と組み合わせた構成により実現しても良い。

【0113】以上のように構成された認証システムの動作について図13を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数 n をともなう場合について説明する。

【0114】まず、クライアント手段41及び認証サーバ手段42において、第1、第2の送受信手段311、321、入力手段312、チケット保持手段314、処理選択手段315、認証情報蓄積手段323、乱数生成手段324の動作は図5、図6の場合と同様であり、認証要求Authenticate Request301及び認証チャレンジChallenge302が交換されて、クライアント手段41においてはユーザ認証処理起動通知4101または利用認可手順起動通知3104が、認証サーバ手段42においては有効回数4201とサーバ識別子3203とパスワード3204と検索結果通知4202とチャレンジ乱数3206とが得られる。ただし、ユーザ認証処理起動通知4101が前記入力手段312、認証用乱数生成手段411及び第1の排他的論理和手段412に送られる点、有効回数4201が第2の多段ハッシュ手段423及び認証子付加手段328に送られる点、検索結果通知4202が第2のハッシュ手段421、乱数生成手段324及びチケット識別子生成手段327に送られる点、チャレンジ乱数3206が第2のハッシュ手段421に送られるとともに第2の送受信手段321を介してクライアント手段41に送られる点が異なる。

【0115】次に、クライアント手段41において、認証

用乱数生成手段411は、ユーザ認証処理起動通知4101が与えられると、認証済み証明に用いられる認証用乱数4102を新たにランダムかつ秘密裏に生成して第1の排他的論理和手段412及び機密記憶手段316に送る（ST4101）。機密記憶手段316は、認証用乱数4102を秘密裏に記憶して所定のアクセスのみ、すなわちユーザ認証手順における追加更新及び利用認可手順における参照のみ許容する（ST4102）。第1の排他的論理和手段412は、ユーザ認証処理起動通知4101が与えられると、ハッシュ手段313より得たハッシュ値4103と認証用乱数4102との間でビット毎の排他的論理和演算を行ない、結果として得られた攪乱ハッシュ値4104を第1の送受信手段311を介して認証チャレンジ応答Response401として認証サーバ手段42に送る（ST4103、ST4104）。

【0116】これに対して認証サーバ手段42においては、認証チャレンジ応答Response401は第2の送受信手段321で受信され、攪乱ハッシュ値4204が取出されて第2の排他的論理和手段422に送られる（ST4202）。一方で第2のハッシュ手段421は、検索結果通知4202が有りを示す場合に、パスワード3204とチャレンジ乱数3206との連結に対しハッシュ演算Hを行なって、結果のハッシュ値4203を第2の排他的論理和手段422に供給している（ST4201）。第2の排他的論理和手段422は、第2のハッシュ手段421より得たハッシュ値4203と攪乱ハッシュ値4204との間でビット毎の排他的論理和演算を行ない、結果として得られた認証用乱数4205を第2の多段ハッシュ手段423に送る（ST4203）。第2の多段ハッシュ手段423は、認証用乱数4205に対し有効回数4201相当の段数のハッシュ演算Hを行なって、結果の多段ハッシュ値4206を認証子付加手段328に送る（ST4204）。

【0117】以下、チケット識別子生成手段327、認証計時手段322、認証子付加手段328の動作は図4、図5の場合と同様であるが、チケット識別子生成手段327が照合結果3209の代わりに検索結果通知4202を用いる点、認証子付加手段328が有効回数3202及び多段ハッシュ値3210の代わりに有効回数4201及び多段ハッシュ値4206を用いる点が異なり、認証チケットデータ3213とは異なる内容の認証チケットデータ4207が得られ（ST4205）、第2の送受信手段321を介して認証チケットTicket402としてクライアント手段41に送られる。

【0118】これに対してクライアント手段41においては、前記第1の送受信手段311、前記チケット保持手段314が図5、図6の場合と同様に動作し、利用認可手順起動通知3104が与えられた場合に、認証チケットTicket403が認可要求Authorize Requestとともに認可サーバ手段33に送られ、有効回数3112が多段ハッシュ手段317に供給される。

【0119】これに対する認可サーバ手段33の動作も図5、図6の場合と同様であり、認可チャレンジChalleng

e306が返される。

【0120】これに対してクライアント手段41においては、前記第1の送受信手段311、多段ハッシュ手段317が図5、図6の場合と同様に動作する。ただし、前記機密記憶手段316より得るのは認証用乱数4105であり（ST4105）、これに対して処理が行なわれる。すなわち、多段ハッシュ手段317が有効回数3112と利用回数3115との差に相当する段数のハッシュ演算Hを行なって（ST4106）、結果の多段ハッシュ値4106を第1の送受信手段311を介して認可チャレンジ応答Response404として認可サーバ手段33に送る（ST4107）。

【0121】これにより認可サーバ手段33が得る認可チャレンジ応答Response404がともなう多段ハッシュ値、認証チケットTicket403がともなう多段ハッシュ値は、図5、図6の場合とはハッシュ対象が異なるのみであり、前者と後者の演算関係は保たれている。従って、これに対する認可サーバ手段33の動作も図5、図6の場合と同様でよく、2つの多段ハッシュ値の関係をチェックして、正当と認めれば認可通知Result308が返され、クライアント手段41において受信される。この方法により、クライアント手段41はパスワードPWを認可サーバ手段33を含めた第三者に明かすことなく、かつパスワードPWとは無関係で安全性のより高い認証チケット402を使用してn回まで利用認可を得ることができる。

【0122】なお、以上の説明ではクライアント手段41において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【0123】このように、認証システムがこの実施形態の構成を採ることにより、クライアント側が計算処理能力の低い装置であっても、実用的な処理時間で利用認可処理を行なうことが可能になる。また、認証チケットに含まれる照合情報がユーザ認証情報と無関係になるため、認証チケットからユーザ認証情報が推測される可能性が無くなり、より安全性の高い、シングルサインオン型の認証方法及び認証システムが得られる。

【0124】（第6の実施の形態）第6の実施形態の認証システムでは、認可サーバからクライアント手段に、認可通知とともに、利用回数が更新された認証チケットが送られる。

【0125】図14は、この認証システムのプロトコルを示すプロトコルシーケンス図である。図14において図4と異なるのは、クライアント手段51及び認可サーバ手段53であって、認証サーバ手段32は変わらない。また、認可サーバ53からクライアント手段51に、認可通知Result308とともに更新された認証チケットTicket501が

送られる点が異なる。

【0126】この認証チケットTicket501は、認証チケット305に比べて、次の点が相違している。

【0127】即ち、認証チケット305での $n+1$ 段ハッシュ演算結果が、 $n-k+1$ 段ハッシュ演算結果（ k は利用回数）に置き換えられている。認証チケット305での有効回数 n が、残り利用可能回数 $n-k$ に置き換えられている。タイムスタンプTS0が新たなタイムスタンプTS k に置き換えられている。発行者識別子IIDが認可サーバ53自身を示すサーバ識別子に置き換えられている。さらに、新たな認証子が付加されている。

【0128】この方法により、クライアント手段51は、パスワードPWを認可サーバ手段53を含めた第三者に明かすことなく、 n 回まで認証チケット304や更新された認証チケット501を使用して利用認可を得ることができる。また、認証チケットのタイムスタンプが毎回更新されるため有効期限をより短く設定できる。そのため、不正な第三者による攻撃対象になりうる期間が短くなり、より安全性が高い。また、認可サーバ手段53におけるハッシュ演算が1段で良いため、利用認可手順における応答時間が短縮できる。

【0129】このようなプロトコルシーケンスを持つ認証システムの構成について図15を参照しながら説明する。

【0130】図15において、図5と異なるのは、クライアント手段51及び認可サーバ手段53であり、認証サーバ手段32は変わらない。また、クライアント手段51において図5のクライアント手段31と異なるのは、チケット保持手段511が認可サーバ手段53からの認証チケットTicket501の認証チケットデータ5101も保持できるようにした点にある。また、認可サーバ手段53において図5の認可サーバ手段33と異なるのは、チケット利用管理手段531が残り利用可能回数をも出力するものとし、第3の多段ハッシュ手段336の代わりに1段のハッシュ演算Hを行なう第3のハッシュ手段532を設け、認証チケットに対する認証子を生成して付加する第2の認証子付加手段533を新たに設け、一部の結線を改めた点にある。

【0131】このチケット保持手段511としては、チケット保持手段314と同様の構成が結線を追加して使用できる。チケット利用管理手段531としては、チケット利用管理手段335と同様の構成が結線を追加して使用できる。第3のハッシュ手段532としては、例えばハッシュ演算Hのアルゴリズムを組み込んだ演算回路が使用できる。第2の認証子付加手段533としては、認証子付加手段328と同様の構成が使用できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【0132】以上のように構成された認証システムの動作について図16を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数 n をとまう場合について説明する。

【0133】まず、クライアント手段51及び認証サーバ手段32における動作は図5、図6の場合と同様で、ユーザ認証手順が行なわれて最終的には、認証サーバ手段32よりクライアント手段51へ認証チケットTicket304が送られる。

【0134】これに対してクライアント手段51においては、第1の送受信手段311は図5、図6の場合と同様に動作し、チケット保持手段511は図5、図6の場合のチケット保持手段314と同様に動作し、認証チケットTicket305が認可要求Authorize Requestとともに認可サーバ手段53に送られるとともに、認証チケットデータから有効回数3112が取出され多段ハッシュ手段317に送られる。

【0135】これに対して認可サーバ手段53においては、第3の送受信手段331、認可計時手段332、認証子検証手段333及びチケット有効判定手段334は図5、図6の場合と同様に動作し、チケット識別子3305と多段ハッシュ値3306と有効回数3307と発行者識別子3308とチケット有効通知3310とをチケット利用管理手段531に供給する。チケット利用管理手段531は、図5、図6の場合のチケット利用管理手段335とほぼ同様に動作して、利用回数5301を第3の送受信手段331を介して認可チャレンジChallenge306としてクライアント手段51に送り、多段ハッシュ値3306をそのまま多段ハッシュ値5302として認可照合手段337に送るが、さらにチケット識別子と残り利用可能回数とサーバ識別子の組5303を出力して第2の認証子付加手段533に送る。

【0136】これに対するクライアント手段51の動作も図5、図6の場合と同様であり、認可チャレンジChallenge306に対して認可チャレンジ応答Response307が返される。

【0137】これに対して認可サーバ手段53においては、認可チャレンジ応答Response307は第3の送受信手段331で受信され、多段ハッシュ値5304が取出されて第3のハッシュ手段532及び第2の認証子付加手段533に送られる。第3のハッシュ手段532は、多段ハッシュ値5304にハッシュ演算 H を行なって、ハッシュの段数が1増えた二次多段ハッシュ値5305を認可照合手段337に送る（ST5301）。認可照合手段337は、多段ハッシュ値5302と二次多段ハッシュ値5305との一致判定を行ない（ST5302、ST3316）、照合結果5307を第2の認証子付加手段533に送る。

【0138】認可計時手段322は現在時刻を計時しており、現在時刻に基づくタイムスタンプ5306を第2の認証子付加手段533に供給している。第2の認証子付加手段533は、チケット識別子と残り利用可能回数とサーバ識別

子の組5303と多段ハッシュ値5304とタイムスタンプ5306と認可サーバ53自身を示す発行者識別子とを連結し、これに対して認証子を生成して付加して認証チケットデータ5308とし（ST5303）、第3の送受信手段331を介して認証チケットTicket501として認可通知Result308とともにクライアント手段51に送る（ST5304）。

【0139】これに対してクライアント手段51においては、認証チケットTicket501は第1の送受信手段311で受信され、認証チケットデータ5101として前記チケット保持手段511に送られ保持されて（ST5101、ST5102）、次回の利用認可手順で使用される。

【0140】これによりクライアント手段51から認可サーバ手段53に送られる認証チケット305がともなう多段ハッシュ値は、その段数が利用認可ごとに1ずつ減って行くので、認可サーバ手段53ではハッシュ演算は1段のみ行なえば良く、応答時間が短縮できる。また、タイムスタンプが更新されるため有効期限をアクセスの間隔をカバーできる程度の短さ、例えば1時間に設定でき、ユーザ利便性は低下させずに安全性を高めることができる。この方法により、クライアント手段31はパスワードPWを認可サーバ手段53を含めた第三者に明かすことなく、安全性のより高い認証チケット305を使用して n 回までより短い応答時間で利用認可を得ることができる。

【0141】なお、以上の説明ではクライアント手段51において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【0142】このように、本実施の形態の認証システムでは、第三者による不正使用の可能性をより小さくでき、また、利用認可の応答時間を短縮することができる。

【0143】（第7の実施の形態）第7の実施形態の認証システムは、認証チケットを複数の認可サーバに対して共通に用いることができる。

【0144】図17は、この認証システムのプロトコルを示すプロトコルシーケンス図である。図17において図4と異なるのは、クライアント手段61、認証サーバ手段62、認可サーバ手段63であって、さらに認証チケット管理手段64を追加している。また、認証チャレンジ応答Response303を受けた認証サーバ手段62が認証要求Authenticate Request301から取出したチケット識別子TIDとサーバ識別子SIDと有効回数 n をとまう認証チケット発行登録指示Registration601を認証チケット管理手段64へ送る点、認可要求Authorize Request602が利用回数 k をとまう点、認可要求Authorize Request602及び認証チケットTicket305を受けた認可サーバ手段6

3が認可要求Authorize Request602及び認証チケット305から取出したチケット識別子TIDとサーバ識別子SIDと利用回数kとをともなった認証チケット履歴更新指示Update603を認証チケット管理手段64へ送る点、これに対して必要に応じて認証チケット拒絶通知Reject606が返される点、認可チャレンジChallenge604が利用回数kの代わりに毎回異なるよう生成された乱数Rkをとともなう点、認可チャレンジ応答Response605がパスワードPWと乱数R0との連結に対して $n-k+1$ 段のハッシュ演算Hを施した結果にさらにRkとの排他的論理和演算を行なった結果をとともなう点が異なる。

【0145】この方法により、クライアント手段61は、パスワードPWを認可サーバ手段63を含めた第三者に明かすことなく、n回まで認証チケット304を使用して利用認可を得ることができ、利用回数kをクライアント手段61から送って認可サーバ手段63とは独立した認証チケット管理手段64でチェックするため、認証チケット304を複数の認可サーバ手段63で共通に利用可能とすることができる。

【0146】このプロトコルシーケンスを持つ認証システムの構成について図18を参照しながら説明する。図18においても図5と異なるのは、クライアント手段61、認証サーバ手段62、及び認可サーバ手段63であって、さらに認証チケット管理手段64を追加している。また、クライアント手段61において図5のクライアント手段31と異なるのは、認証チケットを保持するとともにその利用回数kを管理するチケット保持管理手段611をチケット保持手段314の代わりに設け、ビット毎の排他的論理和演算を行なう第1の排他的論理和手段612を設け、一部の結線を改めた点にある。また、認証サーバ手段62において図5の認証サーバ手段32と異なるのは、認証チケット発行登録指示データを生成するチケット登録指示手段621を設け、一部の結線を改めた点にある。

【0147】また、認可サーバ手段63において図5の認可サーバ手段33と異なるのは、認証チケットのチケット識別子と有効回数と残り利用可能回数を受取って各部に供給するとともに認証チケット履歴更新指示データを生成するチケット更新指示手段631をチケット利用管理手段335の代わりに設け、利用認可処理毎に乱数を生成する第2の乱数生成手段632、ビット毎の排他的論理和演算を行なう第2の排他的論理和手段633を設け、一部の結線を改めた点にある。

【0148】このチケット保持管理手段611としては、チケット保持手段335と同様の構成に利用回数の計算を行なう加算回路を追加して構成される。第1、第2の排他的論理和手段612、633としては、例えば論理回路が使用できる。チケット登録指示手段621としては、例えば論理回路が使用できる。チケット更新指示手段631としては、例えば論理回路が使用できる。第2の乱数生成手段632としては、乱数生成手段324と同様の構成が使用で

きる。認証チケット管理手段64としては、各種通信インタフェース装置とデータの分割結合を行なう論理回路と利用回数を照合する演算回路及び比較回路と大容量のメモリデバイスとの組合せにより構成できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読み取り装置と組み合わせた構成により実現しても良い。

【0149】以上のように構成された認証システムの動作について図19を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数nをとともなう場合について説明する。

【0150】まず、ユーザ認証手順におけるクライアント手段61及び認証サーバ手段62における動作は図5、図6の場合とほぼ同様で、最終的には認証サーバ手段62よりクライアント手段61へ認証チケットTicket304が送られる。ただし、クライアント手段61においては、このときのチケット保持手段314の動作をチケット保持管理手段611が行なう。また認証サーバ手段62においては、認証要求Authenticate Request301から取出された有効回数6201は多段ハッシュ手段325及び認証子付加手段328のほかチケット登録指示手段621にも送られ、サーバ識別子6202は認証子付加手段328のほかチケット登録指示手段621にも送られ、チケット識別子生成手段327で生成されたチケット識別子6203は認証子付加手段328のほかチケット登録指示手段621にも送られる。

【0151】チケット登録指示手段621は、チケット識別子6203とサーバ識別子6202と有効回数6201とを連結して認証チケット発行登録指示データ6204を生成し、第2の送受信手段321を介して認証チケット発行登録指示Registration601として認証チケット管理手段64に送る(ST6201)。これを受けた認証チケット管理手段64はチケットリストを管理しており、認証チケット発行登録指示Registration601が与えられた場合に、チケット識別子を用いてチケットリスト中を検索して既に登録されているかを調べる。該当するものが無ければチケット識別子と有効回数と残り利用可能回数を示す値としての有効回数の組をチケットリストに追加し記憶する。

【0152】これに対してクライアント手段61においては、認証チケットTicket304は第1の送受信手段311で受信され、認証チケットデータ3110が取出されてチケット保持管理手段611に送られる。チケット保持管理手段611は認証チケットデータ3110をサーバ識別子3101と対応づけて保持し、認証チケットデータから取出した有効回数と残り利用可能回数として同時に管理し(ST6101)、利用認可手順起動通知6101が与えられた場合に、認証チケットデータ3111を第1の送受信手段311を介して認証チケットTicket305として、また、残り利用可能

回数を1減じたうえで認証チケットから取出した有効回数から引くことにより得た利用回数6102を（ST6102）第1の送受信手段311を介して認可要求Authorize Request602として、認可サーバ手段63に送り（ST6103）、さらに、認証チケットデータから取出した有効回数3112を多段ハッシュ手段317に送る。

【0153】これに対して認可サーバ手段63においては、認証チケットTicket305及び認可要求Authorize Request602は第3の送受信手段331で受信され、認証チケットデータ3301が取出されて認証子検証手段333に送られ、利用回数6301が取出されてチケット更新指示手段631に送られる（ST6301）。認可計時手段332、認証子検証手段333及びチケット有効判定手段334は図5、図6の場合とほぼ同様に動作し、ただし、サーバ識別子6302はチケット有効判定手段334のほかチケット更新指示手段631にも送られ、有効通知6303はチケット更新指示手段631及び第2の乱数生成手段632に送られる。チケット更新指示手段631は、有効通知6303が与えられると、チケット識別子3305とサーバ識別子6302と利用回数6301とを連結して認証チケット履歴更新指示データ6304を生成し、第3の送受信手段331を介して認証チケット履歴更新指示Update603として認証チケット管理手段64に送る（ST6302）とともに、利用回数6301をそのまま利用回数6306として第3の多段ハッシュ手段336へ送る。認証チケット管理手段64は、認証チケット履歴更新指示Update603が与えられた場合に、チケット識別子を用いてチケットリスト中を検索し、対応する有効回数を示す値が、対応する残り利用可能回数を示す値と認証チケット履歴更新指示Update603がともなう利用回数との合計に一致することをチェックして、正しければチケットリスト中の残り利用可能回数を示す値を1減じ、正しければ認証チケット拒絶通知Reject606を送り返す。認証チケット拒絶通知606は認可サーバ手段63において、第3の送受信手段331を介して認証チケット拒絶通知データ6305として前記チケット更新指示手段631に送られる。チケット更新指示手段631は、多段ハッシュ値3306をそのまま多段ハッシュ値3312として認可照合手段337に送るが、認証チケット拒絶通知データ6305が与えられるとこれを抑止する。第2の乱数生成手段632は、有効通知6303が与えられると、データ攪乱用のチャレンジ乱数6307を新たにランダムに生成して第2の排他的論理和手段633に送るとともに、第3の送受信手段331を介して認可チャレンジChallenge604としてクライアント手段61に送る（ST6303）。

【0154】これに対してクライアント手段61においては、認可チャレンジChallenge604は第1の送受信手段311で受信され、チャレンジ乱数6103が取出されて第1の排他的論理和手段612に送られる（ST6104）。多段ハッシュ手段317は、利用認可手順起動通知6101が与えられている場合に、前記機密記憶手段316よりハッシ

ュ値3113を得て、ハッシュ値3113に有効回数3112と利用回数6102との差に相当する段数のハッシュ演算Hを行なって、結果の多段ハッシュ値6104を、第1の排他的論理和手段612に送る。第1の排他的論理和手段612は、利用認可手順起動通知6101が与えられている場合に、多段ハッシュ値6104とチャレンジ乱数6103との間でビット毎の排他的論理和演算を行ない、攪乱多段ハッシュ値6105を生成し、第1の送受信手段311を介して認可チャレンジ応答Response605として認可サーバ手段63に送る（ST6105、ST6106）。ハッシュ演算Hが充分安全な方向性と結果の長さ及びランダム性を持っている限り、この攪乱多段ハッシュ値6105はパスワードPW、乱数R0及びチャレンジ乱数を知らない第三者には計算することができないため、この攪乱多段ハッシュ値6105によりパスワードPWを知る正当なユーザであることが示される。また、過去にさかのぼるほど多段ハッシュ値におけるハッシュ演算Hの段数が多く行なわれているため、この多段ハッシュ値6104から次の多段ハッシュ値を計算することもできないので、暗号化の必要もない。なお、ハッシュ演算は一般に暗号演算よりも100倍以上高速であるとされ、適切な段数であれば暗号を用いた場合よりも高速に処理が行なえる。

【0155】これに対して認可サーバ手段63においては、認可チャレンジ応答Response605は第3の送受信手段331で受信され、攪乱多段ハッシュ値6308が取出されて第2の排他的論理和手段633に送られる（ST6304）。第2の排他的論理和手段633は、チャレンジ乱数6307と攪乱多段ハッシュ値6308との間でビット毎の排他的論理和演算を行なって、多段ハッシュ値6309を得て第3の多段ハッシュ手段336に送る（ST6305）。第3の多段ハッシュ手段336は、多段ハッシュ値6309に利用回数6306に相当する段数のハッシュ演算を行なって、結果の二次多段ハッシュ値3314を認可照合手段337に送る。認可照合手段337は図5、図6の場合と同様に動作し、認可通知データ3315を第3の送受信手段331を介して認可通知Result308としてクライアント手段61に送り、クライアント手段61において受信される。ただし、認証チケット拒絶通知Reject606の受信により多段ハッシュ値3312の供給が抑止された場合にはこの限りではない（ST6306、ST6307）。この方法により、クライアント手段61はパスワードPWを認可サーバ手段63を含めた第三者に明かすことなく、n回まで認証チケット305を使用して複数の認可サーバ手段に対して利用認可を得ることができる。

【0156】なお、以上の説明ではクライアント手段61において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる

必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【0157】このように、この実施形態では、認証チケットが更新されない方式の下で、認証チケットを複数の認可サーバに対して共通に用いることができる、利便性の高いシングルサインオン型の認証システムを構成することができる。

【0158】（第8の実施の形態）第8の実施形態の認証システムは、認証チケットの利用を分散管理することができる。

【0159】図20は、この認証システムのプロトコルを示すプロトコルシーケンス図である。図20において図14と異なるのは、クライアント手段71、認証サーバ手段72及び認可サーバ手段73であって、さらに第2の認可サーバ手段74を追加している。また、認可要求Authorize Request701が利用回数 k をとともう点、認可要求Authorize Request701及び認証チケットTicket305を受けた認可サーバ手段73が認可要求Authorize Request701及び認証チケット305から取出したチケット識別子TIDとサーバ識別子SIDと利用回数 k をとともなった認証チケット履歴照会Inquiry702を認証サーバ手段72または第2の認可サーバ手段74へ送る点、これに対して必要に応じて認証チケット拒絶通知Reject705が返される点、認可チャレンジChallenge703が利用回数 k の代わりに毎回異なるよう生成された乱数 R_k をとともう点、認可チャレンジ応答Response704がパスワードPWと乱数 R_0 との連結に対して $n-k+1$ 段のハッシュ演算 H を施した結果にさらに R_k との排他的論理和演算を行なった結果をとともう点が異なる。

【0160】この方法により、クライアント手段71はパスワードPWを認可サーバ手段73、第2の認可サーバ手段74を含めた第三者に明かすことなく、 n 回まで認証チケット304や更新された認証チケット501を使用して利用認可を得ることができ、利用回数 k をクライアント手段71から認可サーバ手段73を介して認証チケットを発行した認証サーバ手段72または更新した第2の認可サーバ手段74に送ってチェックするため、認証チケット304を複数の認可サーバ手段73、74で共通に利用可能なものとして、かつチェック処理のトラフィックを分散化できる。

【0161】このようなプロトコルシーケンスを持つ認証システムの構成について図21を参照しながら説明する。図21においても図15と異なるのは、クライアント手段71、認証サーバ手段72、認可サーバ手段73であって、さらに第2の認可サーバ手段74を追加している。また、クライアント手段71において図15のクライアント手段51と異なるのは、認証チケットを保持するとともにその利用回数 k を管理するチケット保持管理手段711をチケット保持手段511の代わりに設け、ビット毎の排他的論理和演算を行なう第1の排他的論理和手段712を設

け、一部の結線を改めた点にある。また、認証サーバ手段72において図15の認証サーバ手段32と異なるのは、認証チケットの発行を管理して照会に回答するチケット発行管理手段721を設け、一部の結線を改めた点にある。また、認可サーバ手段73において図15の認可サーバ手段53と異なるのは、認証チケットのチケット識別子と有効回数と残り利用可能回数とを受取って各部に供給するとともに認証チケットの更新を管理して照会に回答するチケット更新管理手段731をチケット利用管理手段531の代わりに設け、利用認可処理毎に乱数を生成する第2の乱数生成手段732、ビット毎の排他的論理和演算を行なう第2の排他的論理和手段733を設け、一部の結線を改めた点にある。第2の認可サーバ手段74は認可サーバ手段73と同様の構成を持つものである。

【0162】チケット保持管理手段711としては、チケット保持手段511と同様の構成に利用回数の計算を行なう加算回路を追加して使用できる。第1、第2の排他的論理和手段712、733としては、例えば論理回路が使用できる。チケット発行管理手段721としては、例えばデータの分割結合を行なう論理回路と利用回数を照合する演算回路及び比較回路と大容量のメモリデバイスとの組合せにより構成できる。チケット更新管理手段731としては、例えばデータの分割結合を行なう論理回路と利用回数を照合する演算回路及び比較回路と大容量のメモリデバイスとの組合せにより構成できる。第2の乱数生成手段732としては、乱数生成手段324と同様の構成が使用できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読み取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読み取り装置と組み合わせた構成により実現しても良い。

【0163】以上のように構成された認証システムの動作について図22を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数 n をとともう場合について説明する。

【0164】まず、ユーザ認証手順におけるクライアント手段71及び認証サーバ手段72における動作は図15、図16の場合とほぼ同様で、最終的には認証サーバ手段72よりクライアント手段71へ認証チケットTicket304が送られる。ただし、クライアント手段71においては、このときのチケット保持手段511の動作をチケット保持管理手段711が行なう。また認証サーバ手段72においては、認証要求Authenticate Request301から取出された有効回数7201は多段ハッシュ手段325及び認証子付加手段328のほかチケット発行管理手段721にも送られ、サーバ識別子7202は認証子付加手段328のほかチケット発行管理手段721にも送られ、チケット識別子生成手段327で生成されたチケット識別子7203は認証子付加手段328のほかチケット発行管理手段721にも送られる。チケット

発行管理手段721は発行したチケットリストを管理しており、チケット識別子7203とサーバ識別子7202と有効回数7201と残り利用可能回数を示す値としての有効回数7201の組をチケットリストに追加し記憶する（ST7201）。

【0165】これに対してクライアント手段71においては、認証チケットTicket304は第1の送受信手段311で受信され、認証チケットデータ3110が取出されて前記チケット保持管理手段711に送られる。前記チケット保持管理手段711は、認証チケットデータ3110をサーバ識別子3101と対応づけて保持し、認証チケットデータから取出した有効回数と残り利用可能回数として同時に管理し（ST7101）、利用認可手順起動通知7101が与えられた場合に、認証チケットデータ3111を第1の送受信手段311を介して認証チケットTicket305として、また、残り利用可能回数を1減じたうえで認証チケットから取出した有効回数から引くことにより得た利用回数7102を（ST7102）第1の送受信手段311を介して認可要求Authorize Request701として、それぞれ認可サーバ手段73に送り（ST7103）、さらに認証チケットデータから取出した有効回数3112を多段ハッシュ手段317に送る。

【0166】これに対して認可サーバ手段73においては、認証チケットTicket305及び認可要求Authorize Request701は第3の送受信手段331で受信され、認証チケットデータ3301が取出されて認証子検証手段333に送られ、利用回数7301が取出されてチケット更新管理手段731に送られる（ST7301）。

【0167】認可計時手段332、認証子検証手段333及びチケット有効判定手段334は図15、図16の場合とほぼ同様に動作し、ただし、サーバ識別子7302はチケット有効判定手段334のほかチケット更新管理手段731にも送られ、有効通知7303はチケット更新管理手段731及び第2の乱数生成手段732に送られる。チケット更新管理手段731は発行したチケットリストを管理しており、有効通知7303が与えられると、チケット識別子3305とサーバ識別子7302と利用回数7301とを連結して認証チケット履歴照会データ7304を得て、第3の送受信手段331を介して発行者識別子3308の示す認証サーバ手段72または第2の認可サーバ手段74へ認証チケット履歴照会Inquiry702を送るとともに、チケット識別子3305とサーバ識別子7302と有効回数7301と残り利用可能回数を示す値としての有効回数7301の組をチケットリストに追加し記憶する（ST7302）。

【0168】これを受けた認証サーバ手段72では、認証チケット履歴照会Inquiry702は第2の送受信手段321で受信され、チケット識別子とサーバ識別子と利用回数とを含んだ認証チケット履歴照会データ7205として前記チケット発行管理手段721に送られる。前記チケット発行管理手段721は、認証チケット履歴照会データ7205から

取出した利用回数が、自ら管理する有効回数と残り利用可能回数との差に1加えたものと一致するかを調べ、不一致の場合には認証チケット拒絶通知データ7204を第2の送受信手段321を介して認証チケット拒絶通知Reject705として送り返す。なお、第2の認可サーバ手段74がこれを受けた場合には、チケット更新管理手段が前記チケット発行管理手段721と同様の役割を行なう。

【0169】認可サーバ手段73においては、認証チケット拒絶通知705は第3の送受信手段331を介して認証チケット拒絶通知データ7305として前記チケット更新管理手段731に送られる。前記チケット更新管理手段731は、多段ハッシュ値3306をそのまま多段ハッシュ値5302として認可照会手段337に送り、チケット識別子と残り利用可能回数とサーバ識別子との組5303を第2の認証子付加手段533に送るが、認証チケット拒絶通知データ7305が与えられるとこれらを抑止する。第2の乱数生成手段732は、有効通知7303が与えられると、データ搅乱用のチャレンジ乱数7306を新たにランダムに生成して第2の排他的論理和手段733に送るとともに、第3の送受信手段331を介して認可チャレンジChallenge703としてクライアント手段71に送る（ST7303）。

【0170】これに対してクライアント手段71においては、認可チャレンジChallenge703は第1の送受信手段311で受信され、チャレンジ乱数7103が取出されて第1の排他的論理和手段712に送られる（ST7104）。多段ハッシュ手段317は、利用認可手順起動通知7101が与えられている場合に、前記機密記憶手段316よりハッシュ値3113を得て、ハッシュ値3113に有効回数3112と利用回数7102との差に相当する段数のハッシュ演算Hを行なって、結果の多段ハッシュ値7104を、第1の排他的論理和手段712に送る。第1の排他的論理和手段712は、利用認可手順起動通知7101が与えられている場合に、多段ハッシュ値7104とチャレンジ乱数7103との間でビット毎の排他的論理和演算を行ない、搅乱多段ハッシュ値7105を生成し、第1の送受信手段311を介して認可チャレンジ応答Response704として認可サーバ手段73に送る（ST7105、ST7106）。ハッシュ演算Hが充分安全な一方向性と結果の長さ及びランダム性を持っている限り、この搅乱多段ハッシュ値7105はパスワードPW、乱数R0及びチャレンジ乱数を知らない第三者には計算することができないため、この搅乱多段ハッシュ値7105によりパスワードPWを知る正当なユーザであることが示される。また、過去にさかのぼるほど多段ハッシュ値におけるハッシュ演算Hの段数が多く行なわれているため、この多段ハッシュ値7104から次の多段ハッシュ値を計算することもできないので、暗号化の必要もない。なお、ハッシュ演算は一般に暗号演算よりも100倍以上高速であるとされ、適切な段数であれば暗号を用いた場合よりも高速に処理が行なえる。

【0171】これに対して認可サーバ手段73において

は、認可チャレンジ応答Response704は第3の送受信手段331で受信され、攪乱多段ハッシュ値7307が取出されて第2の排他的論理和手段733に送られる（ST7304）。第2の排他的論理和手段733は、チャレンジ乱数7306と攪乱多段ハッシュ値7307との間でビット毎の排他的論理和演算を行なって、多段ハッシュ値7308を得て第3のハッシュ手段532に送る（ST7305）。第3のハッシュ手段532は、多段ハッシュ値7308にハッシュ演算を行なって、結果の二次多段ハッシュ値5305を認可照合手段337に送る。認可照合手段337及び第2の認証子付加手段533は図15、図16の場合と同様に動作し、認証チケットデータ5308を第3の送受信手段331を介して認証チケットTicket501としてクライアント手段71に送る。ただし、認証チケット拒絶通知Reject705の受信により多段ハッシュ値5302及びチケット識別子と残り利用可能回数とサーバ識別子との組5303の供給が抑止された場合にはこの限りではない（ST7306、ST7307）。

【0172】これに対してクライアント手段71においては、認証チケットTicket501は第1の送受信手段311で受信され、認証チケットデータ5101として前記チケット保持管理手段711に送られ保持されて（ST7107、ST7108）、次の利用認可手順で使用される。

【0173】これによりクライアント手段71から認可サーバ手段73に送られる認証チケット305がともなう攪乱多段ハッシュ値は、その段数が利用認可ごとに1ずつ減っていくので、認可サーバ手段73ではハッシュ演算は1段のみ行なえば良く、応答時間が短縮できる。また、タイムスタンプが更新されるため有効期限をアクセスの間隔をカバーできる程度の短さ、例えば1時間に設定でき、ユーザ利便性は低下させずに安全性を高めることができる。この方法により、クライアント手段71はパスワードPWを認可サーバ手段73、74を含めた第三者に明かすことなく、安全性のより高い認証チケット305を使用してn回まで、より短い応答時間で利用認可を得ることができ、その認証チケットは複数の認可サーバで共通に利用可能で、かつチェック処理のトラフィックを分散化できる。

【0174】なお、以上の説明ではクライアント手段71において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【0175】このように、認証システムを本実施形態のように構成することにより、認証チケットが更新される方式の下で、認証チケットの利用を分散管理することができる。そのため1個所の管理リソースをより少なくで

きる。

【0176】

【発明の効果】以上の説明から明らかなように、本発明では、第1に、クライアント側での暗号処理を必要とせず、認証チケットの使用回数を容易に管理して二重使用を排除することができる、シングルサインオン型の認証方法及び認証システムが得られる。

【0177】第2に、ユーザ認証手順においても、クライアント側での暗号処理を必要としないいうえ、認証提示情報の演算処理と提示情報の演算処理とが共通化できる、シングルサインオン型の認証方法及び認証システムが得られる。

【0178】第3に、クライアント手段が生成した認証用乱数を秘密情報として照合情報を生成するものでは、認証チケットが含む照合情報がユーザ認証情報と無関係となるため認証チケットからユーザ認証情報が推測される可能性すらなく、より安全性の高いシングルサインオン型の認証方法及び認証システムが得られる。

【0179】第4に、秘密情報の不可逆演算を一方方向性ハッシュ演算で行なうことにより、クライアント側が計算処理能力の低い装置であっても実用的な処理時間で利用認可処理を行なうことができる、シングルサインオン型の認証方法及び認証システムが得られる。

【0180】第5に、認可サーバ手段が認証チケットの照合情報等を更新するものでは、認証チケットが更新することに更新され、特にタイムスタンプが更新されるため有効判定における有効期限をより短く設定できるので、第三者による不正使用の可能性をより小さくでき、さらに利用認可の応答時間を短縮できる、シングルサインオン型の認証方法及び認証システムが得られる。

【0181】第6に、認証チケットの使用回数を管理する認証チケット管理手段を設けたものでは、認証チケットが更新されないシステムにおいて、認証チケットを複数の認可サーバに対して共通に用いることが可能となるため、より利便性の高いシングルサインオン型の認証方法及び認証システムが得られる。

【0182】第7に、認証サーバ手段や認可サーバ手段が認証チケットの発行履歴を記憶するものでは、認証チケットが更新されるシステムにおいて、認証チケットの利用を分散管理できるため1個所の管理リソースをより少なくできる、シングルサインオン型の認証方法及び認証システムが得られる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態における認証システムの概要を示す概念図、

【図2】本発明の第2の実施の形態における認証システムの概要を示す概念図、

【図3】本発明の第3の実施の形態における認証システムの概要を示す概念図、

【図4】本発明の第4の実施の形態における認証システ

ムのプロトコルシーケンス図、

【図 5】本発明の第 4 の実施の形態における認証システム
の機能ブロック図、

【図 6】本発明の第 4 の実施の形態における認証システム
の動作を示すフロー図、

【図 7】本発明の第 4 の実施の形態における認証システム
においてメッセージ認証コードを用いた場合の認証子
付加手段の詳細な機能ブロック図、

【図 8】本発明の第 4 の実施の形態における認証システム
においてメッセージ認証コードを用いた場合の認証子
検証手段の詳細な機能ブロック図、

【図 9】本発明の第 4 の実施の形態における認証システム
においてデジタル署名を用いた場合の認証子付加手段
の詳細な機能ブロック図、

【図 10】本発明の第 4 の実施の形態における認証システム
においてデジタル署名を用いた場合の認証子検証手段
の詳細な機能ブロック図、

【図 11】本発明の第 5 の実施の形態における認証システム
のプロトコルシーケンス図、

【図 12】本発明の第 5 の実施の形態における認証システム
の機能ブロック図、

【図 13】本発明の第 5 の実施の形態における認証システム
の動作を示すフロー図、

【図 14】本発明の第 6 の実施の形態における認証システム
のプロトコルシーケンス図、

【図 15】本発明の第 6 の実施の形態における認証システム
の機能ブロック図、

【図 16】本発明の第 6 の実施の形態における認証システム
の動作を示すフロー図、

【図 17】本発明の第 7 の実施の形態における認証システム
のプロトコルシーケンス図、

【図 18】本発明の第 7 の実施の形態における認証システム
の機能ブロック図、

【図 19】本発明の第 7 の実施の形態における認証システム
の動作を示すフロー図、

【図 20】本発明の第 8 の実施の形態における認証システム
のプロトコルシーケンス図、

【図 21】本発明の第 8 の実施の形態における認証システム
の機能ブロック図、

【図 22】本発明の第 8 の実施の形態における認証システム
の動作を示すフロー図、

【図 23】従来の認証方法の概要を示す概念図、

【図 24】従来の認証方法のプロトコルシーケンス図、

【図 25】従来の認証方法の機能ブロック図、

【図 26】従来の認証方法の動作を示すフロー図である。

【符号の説明】

1、11、21、31、41、51、61、71、81 クライアント手段

2、12、22、32、42、62、72、82 認証サーバ手段

3、33、53、63、73、83 認可サーバ手段

4、14、24 秘密情報

5、7、803、805 認証チケット

6、804 提示情報

8、806 認可通知

13、23、801 認証提示情報

64 認証チケット管理手段

74 第 2 の認可サーバ手段

311 第 1 の送受信手段

312、811 入力手段

313 ハッシュ手段

314 チケット保持手段

316 機密記憶手段

317 多段ハッシュ手段

321 第 2 の送受信手段

322 認証計時手段

323 認証情報蓄積手段

324 乱数生成手段

325 第 2 の多段ハッシュ手段

326 認証照合手段

327 チケット識別子生成手段

328 認証子付加手段

328A 自識別子記憶手段

328B データ連結手段

328C 連結データハッシュ手段

328D サーバ共通鍵記憶手段

328E 共通鍵方式暗号手段

328F 認証子連結手段

328G 自秘密鍵記憶手段

328H 公開鍵方式暗号手段

331 第 3 の送受信手段

332 認可計時手段

333 認証子検証手段

333A 認証子分離手段

333B 第 2 の連結データハッシュ手段

333C 第 2 のサーバ共通鍵記憶手段

333D 第 2 の共通鍵方式暗号手段

333E データ分離手段

333F 発行者識別子照合手段

333G 比較手段

333H サーバ公開鍵蓄積手段

333J 公開鍵方式復号手段

334、832 チケット有効判定手段

335、531 チケット利用管理手段

336 第 3 の多段ハッシュ手段

337 認可照合手段

411 認証用乱数生成手段

412、612、712 第 1 の排他的論理和手段

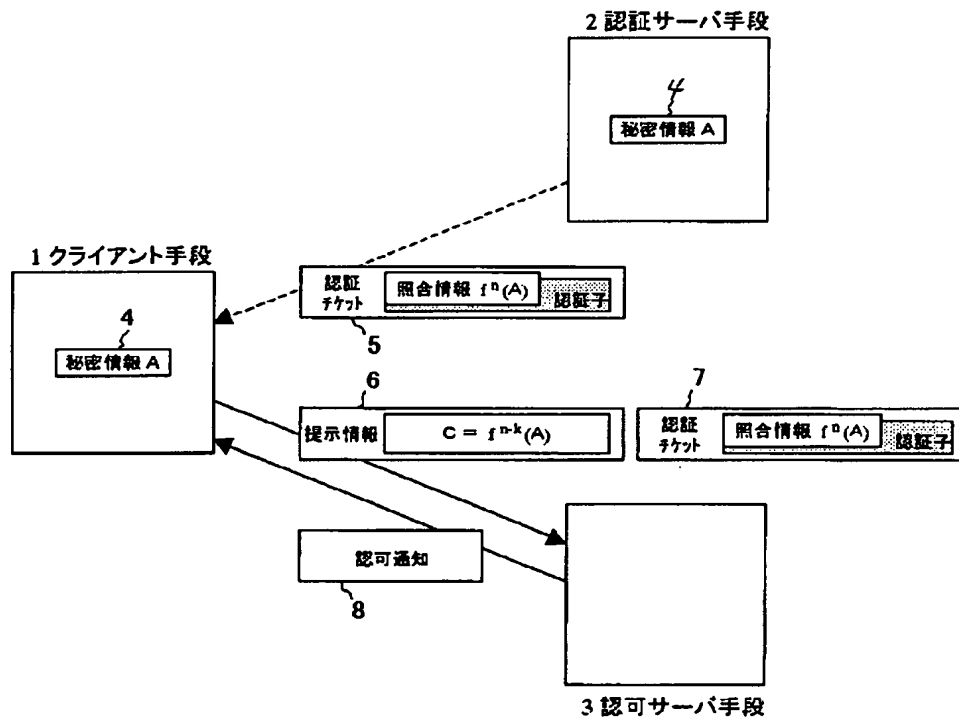
421 第 2 のハッシュ手段

422 第 2 の排他的論理和手段

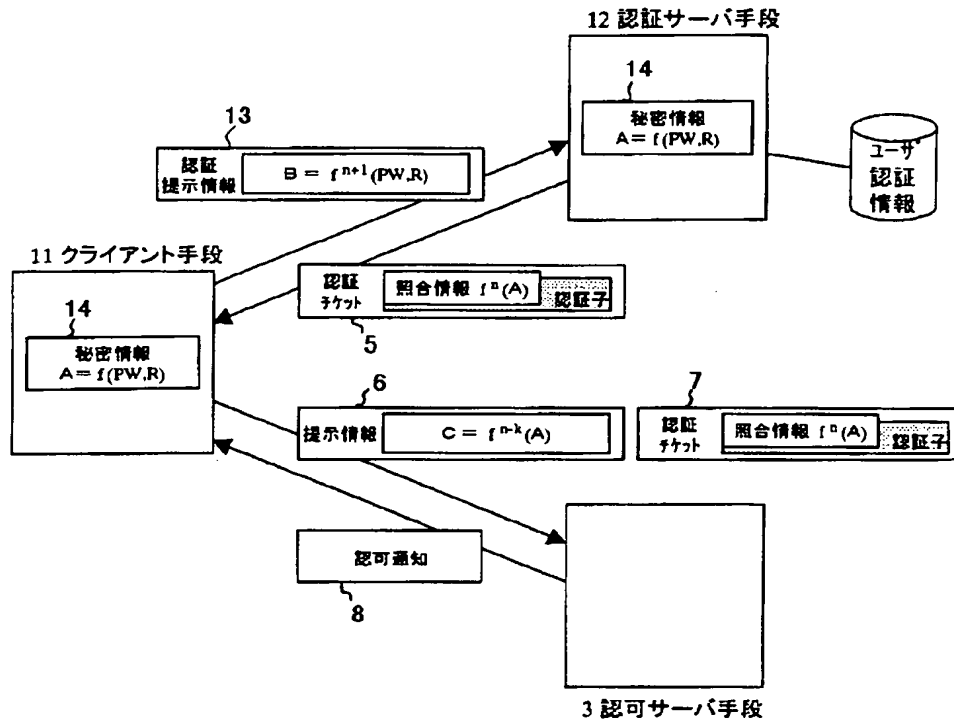
423 第2の多段ハッシュ手段
 511 チケット保持手段
 532 第3のハッシュ手段
 533 第2の認証子付加手段
 611、711 チケット保持管理手段
 621 チケット登録指示手段
 631 チケット更新指示手段
 632 第2の乱数生成手段
 633、733 第2の排他的論理和手段
 721 チケット発行管理手段
 731 チケット更新管理手段

732 第2の乱数生成手段
 812 セッション鍵復号手段
 813 証明計時手段
 814 証明情報暗号手段
 821 セッション鍵生成手段
 822 セッション鍵暗号手段
 823 チケット暗号手段
 831 チケット復号手段
 833 証明情報復号手段
 834 証明情報有効判定手段
 835 認可照合手段

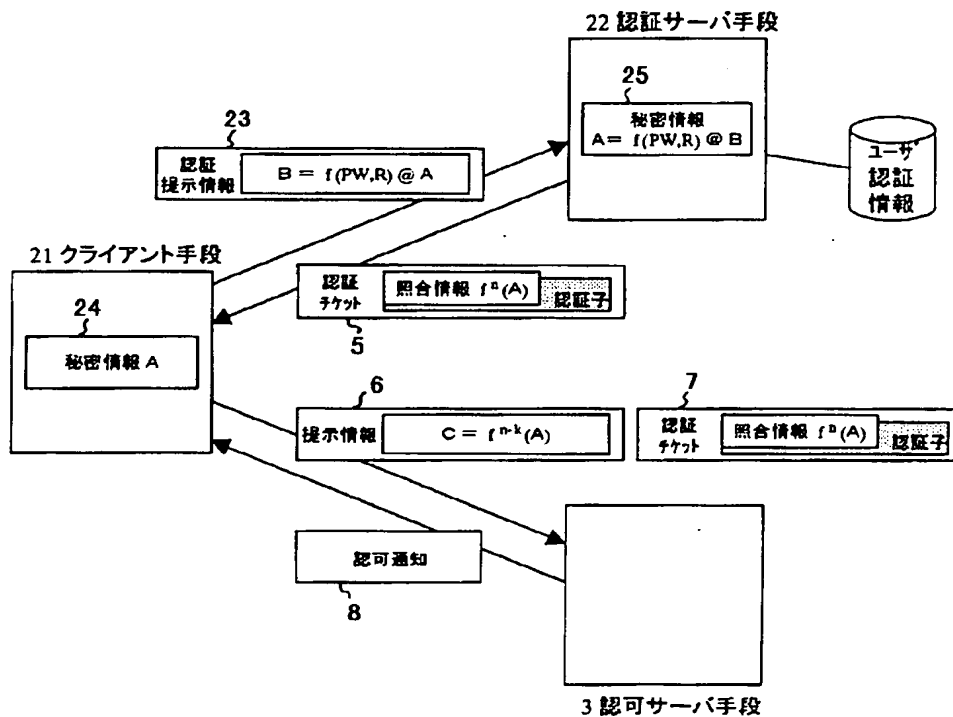
【図1】



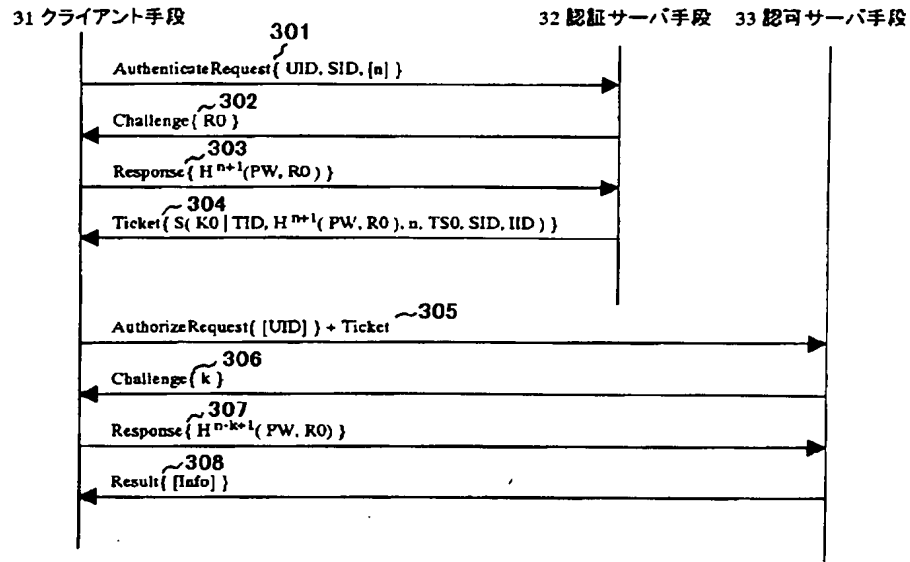
【図2】



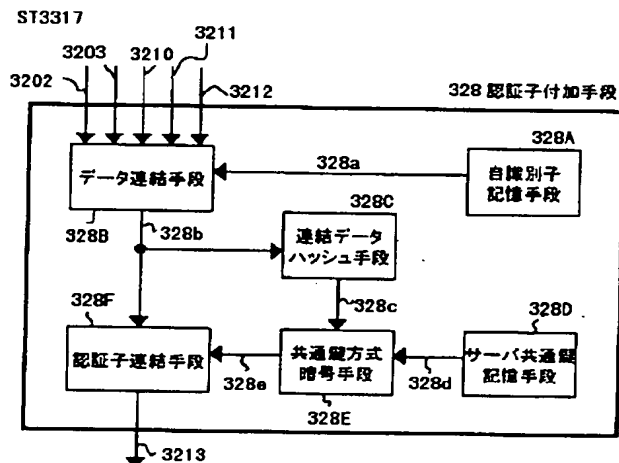
【図3】



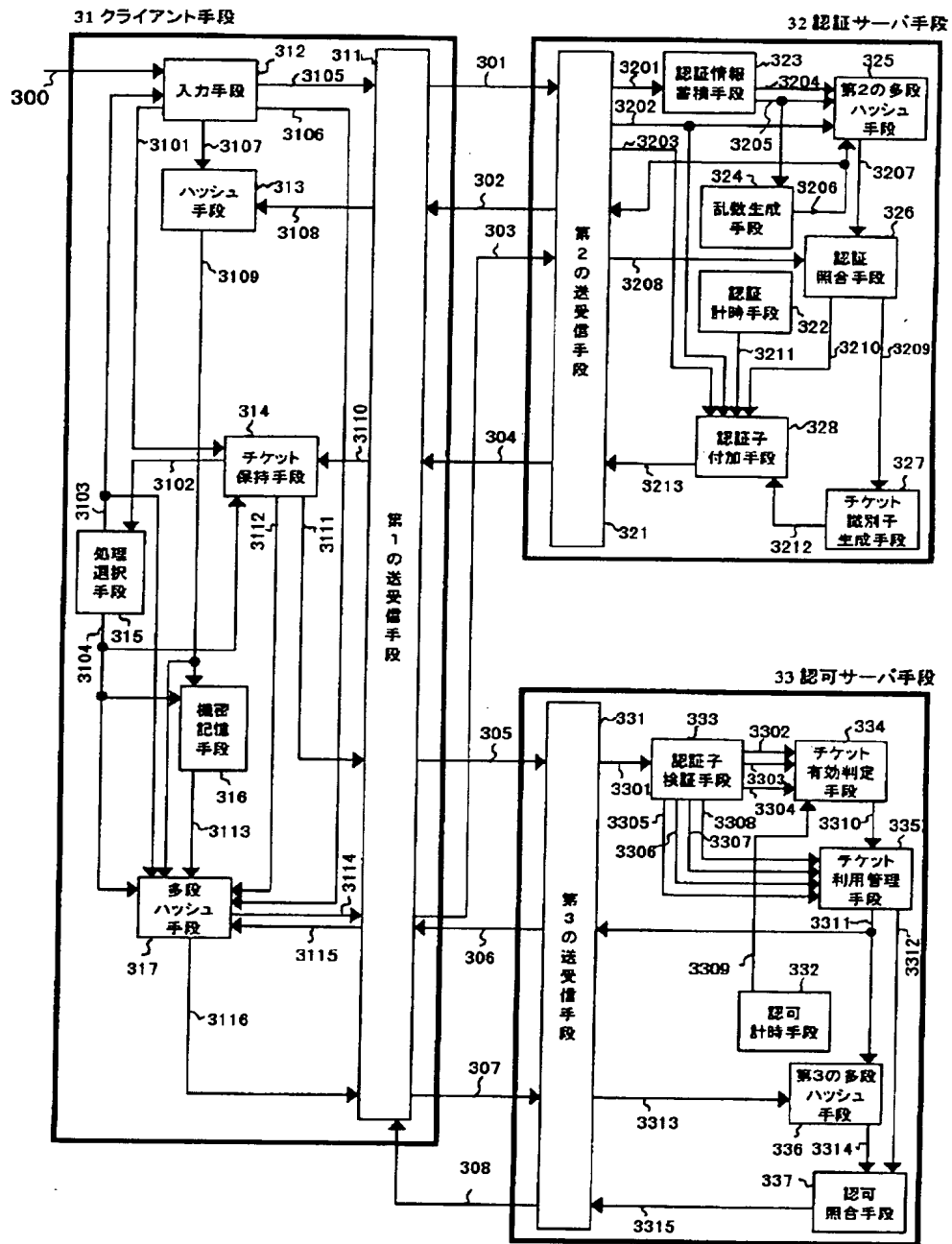
【図4】



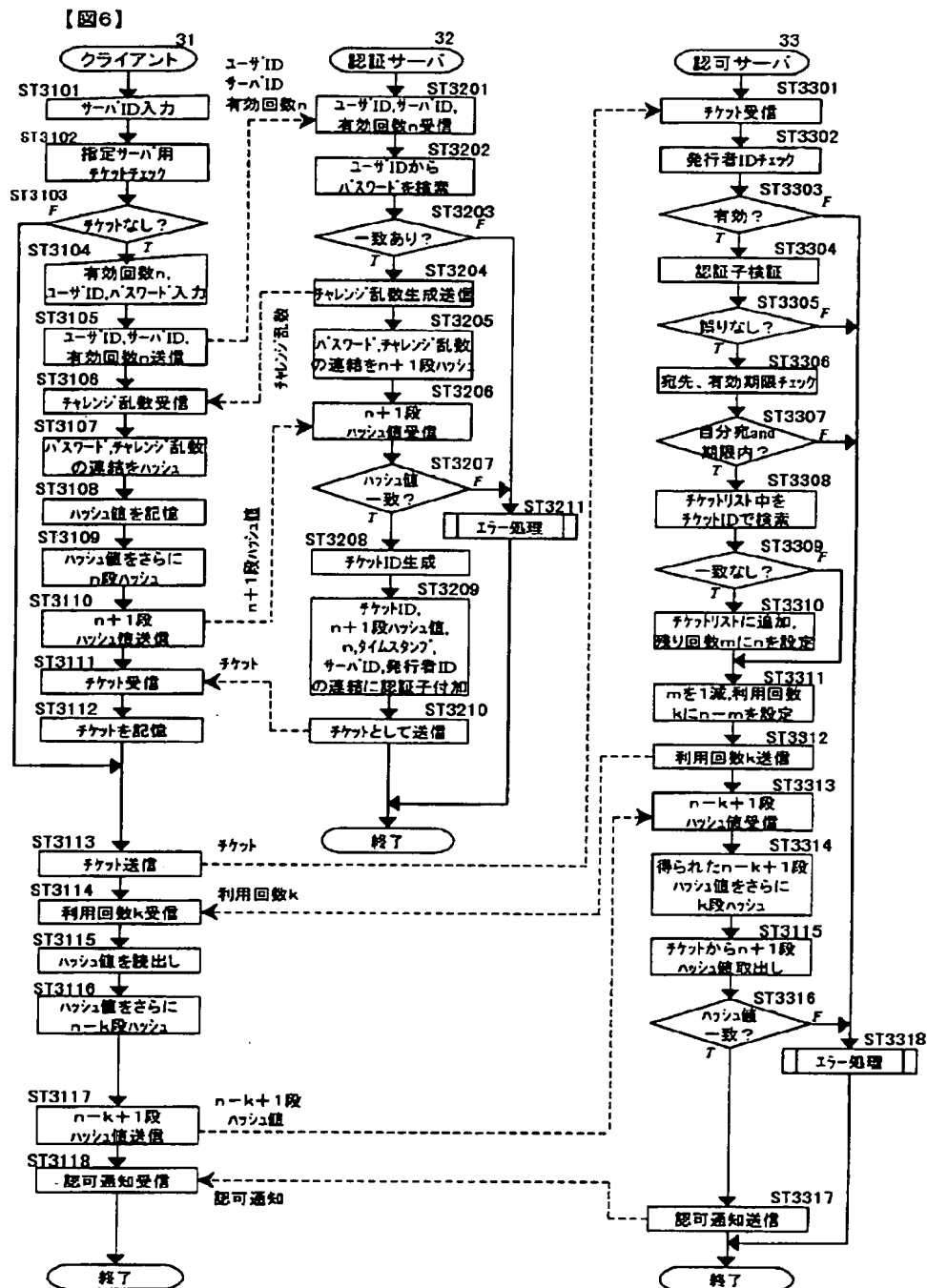
【図7】



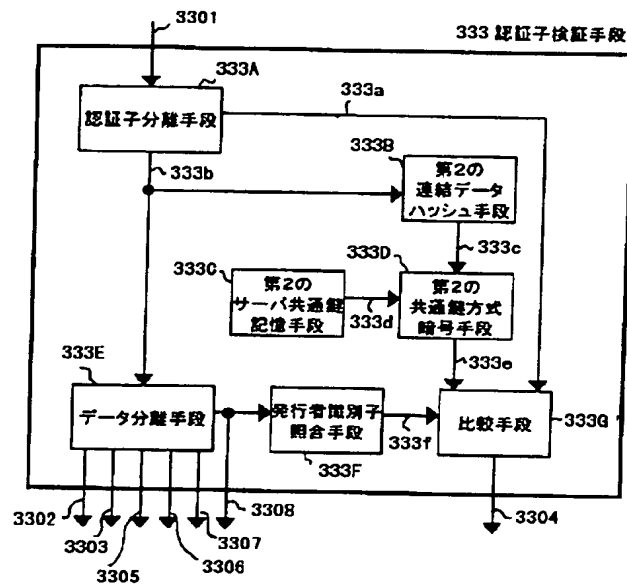
【図5】



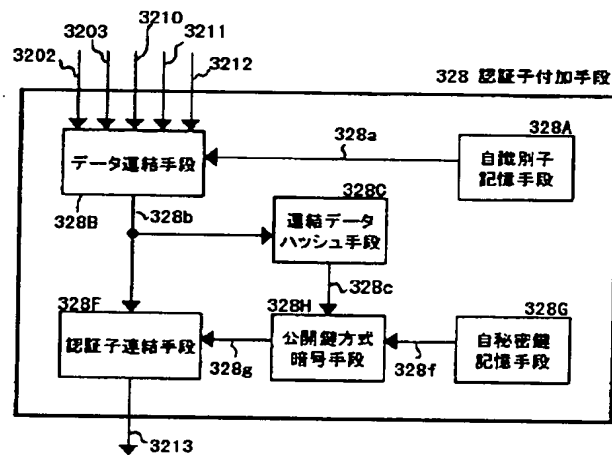
【図6】



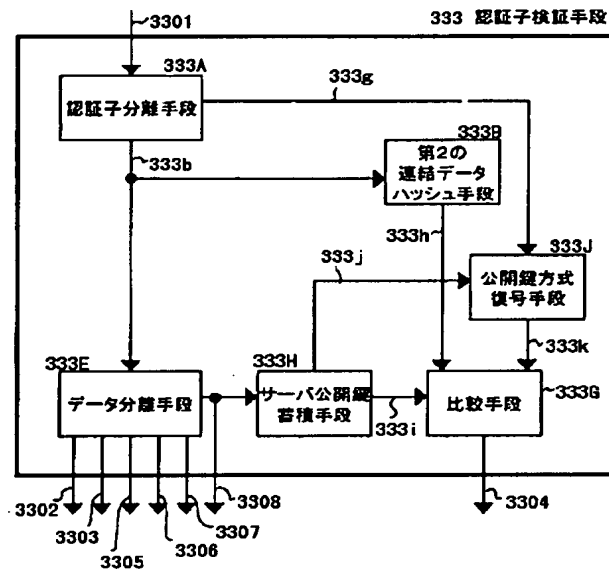
【図8】



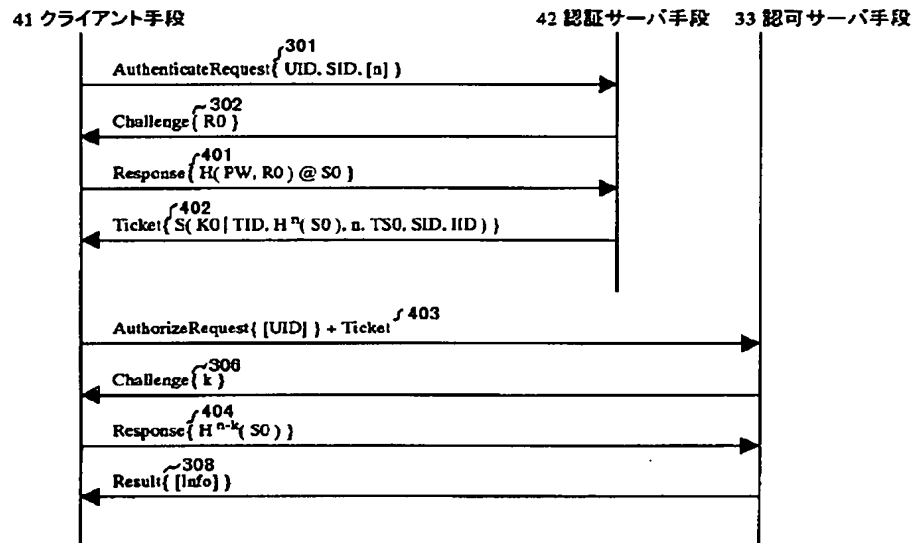
【図9】



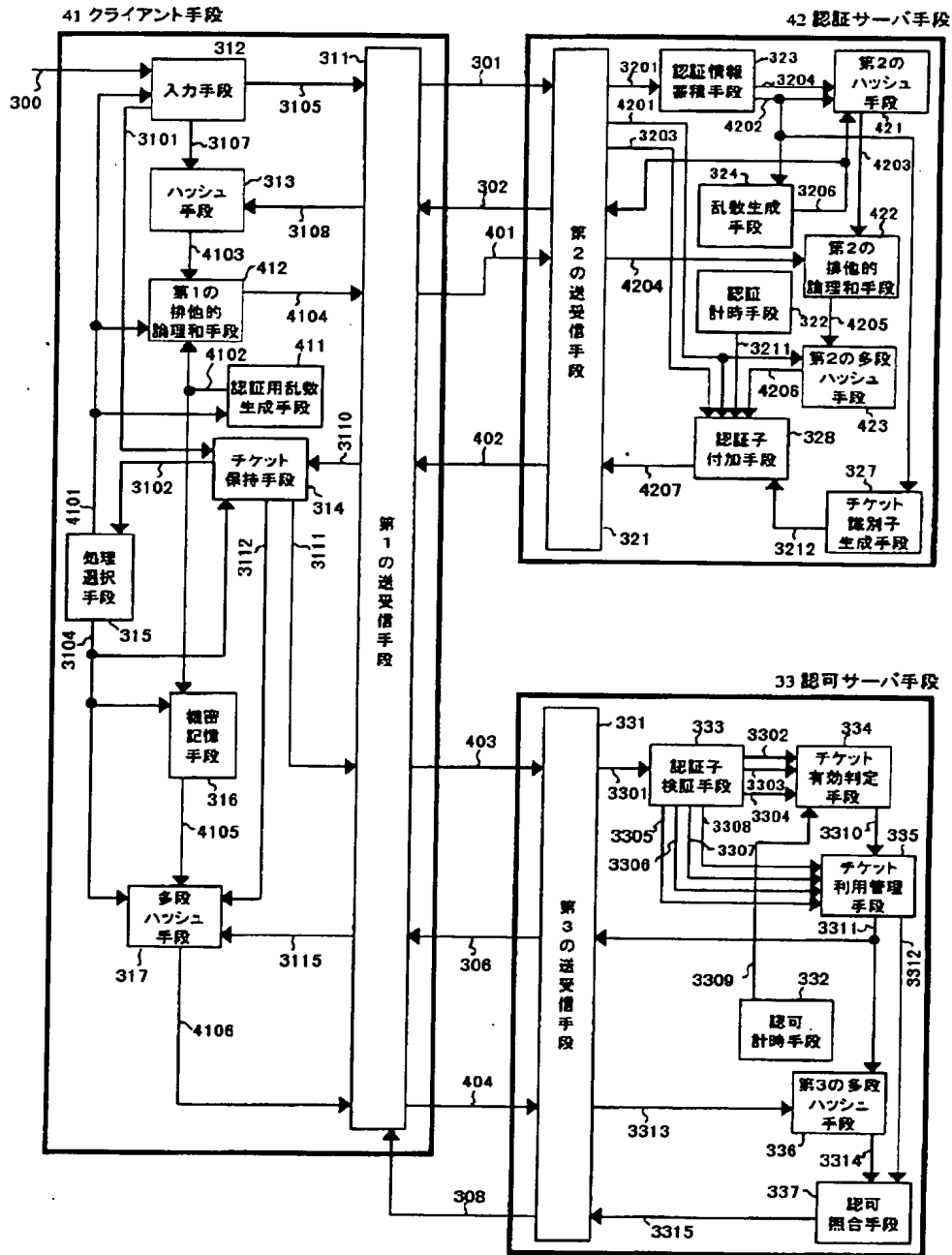
【図10】



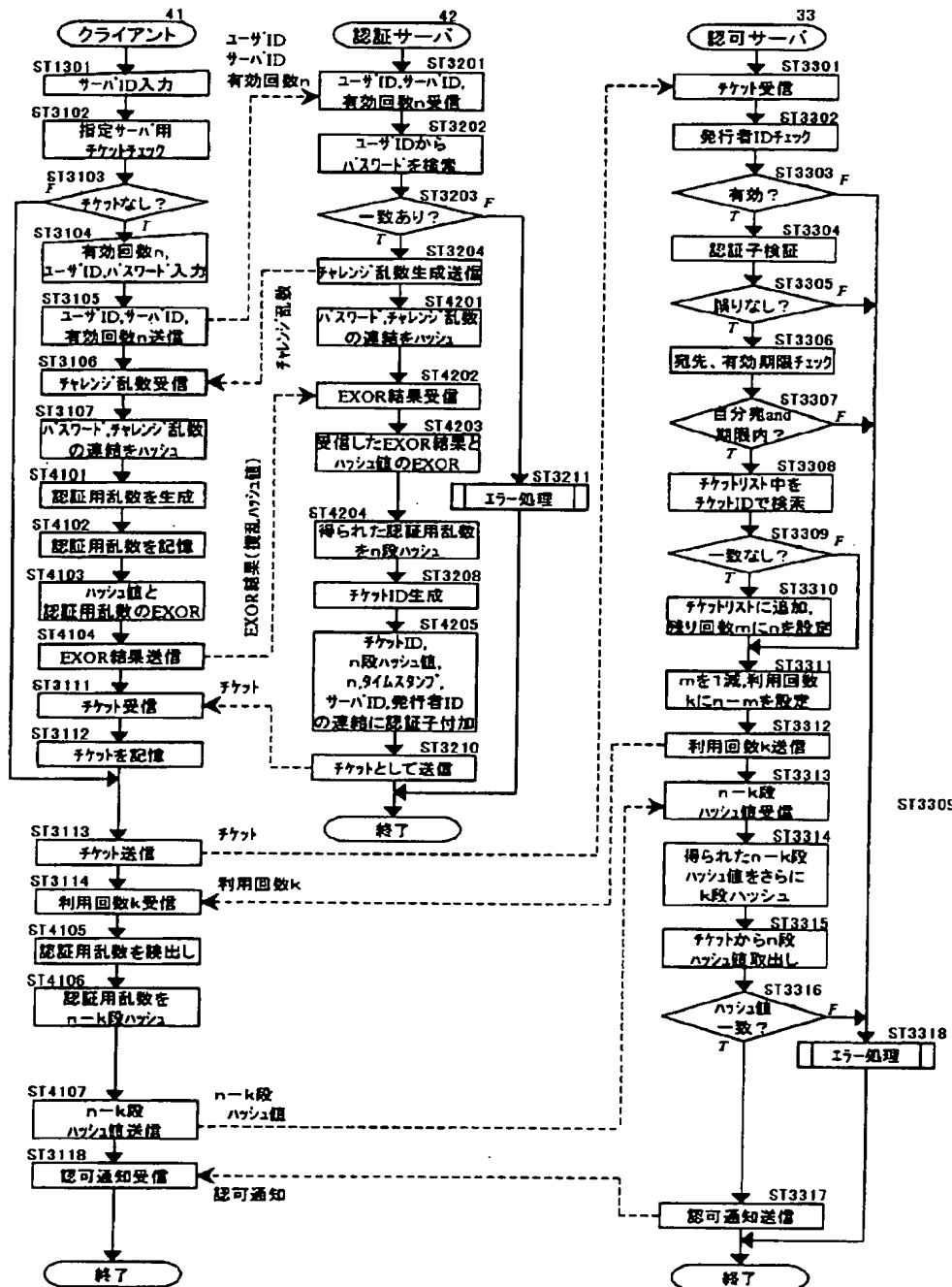
【図11】



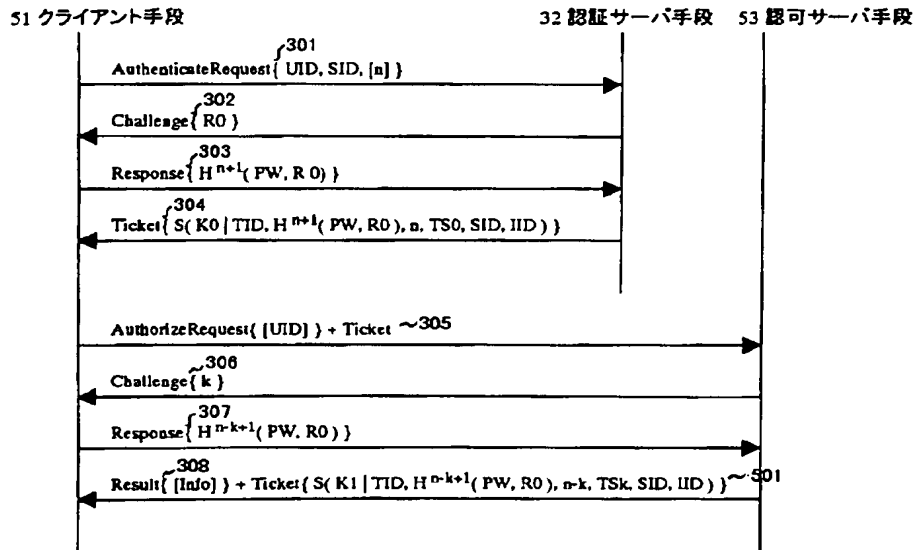
【図12】



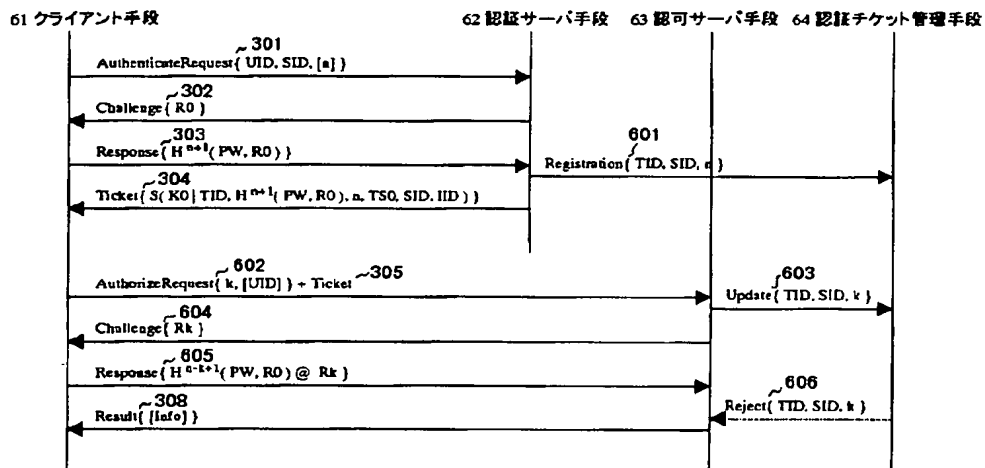
【図13】



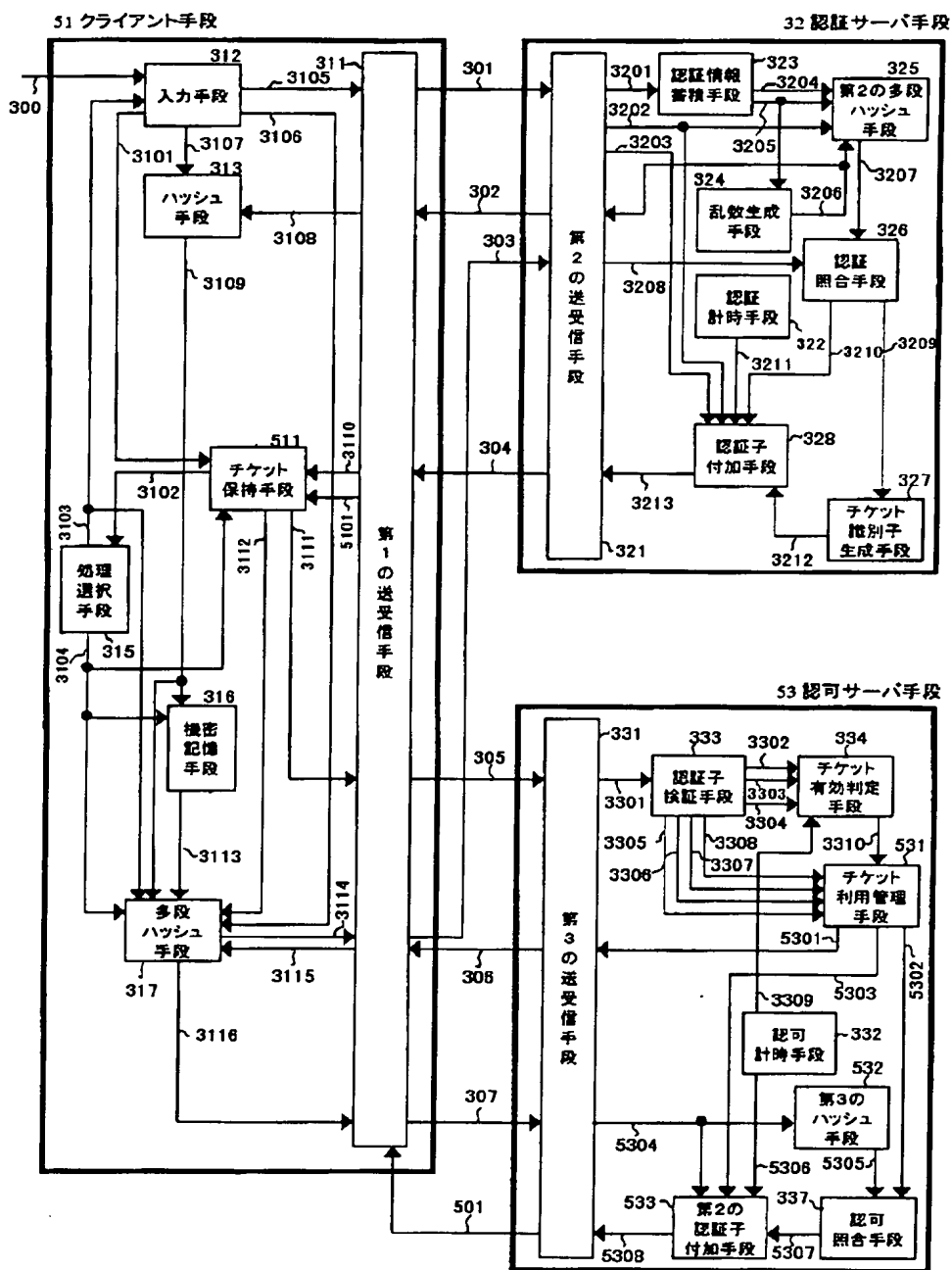
【図14】



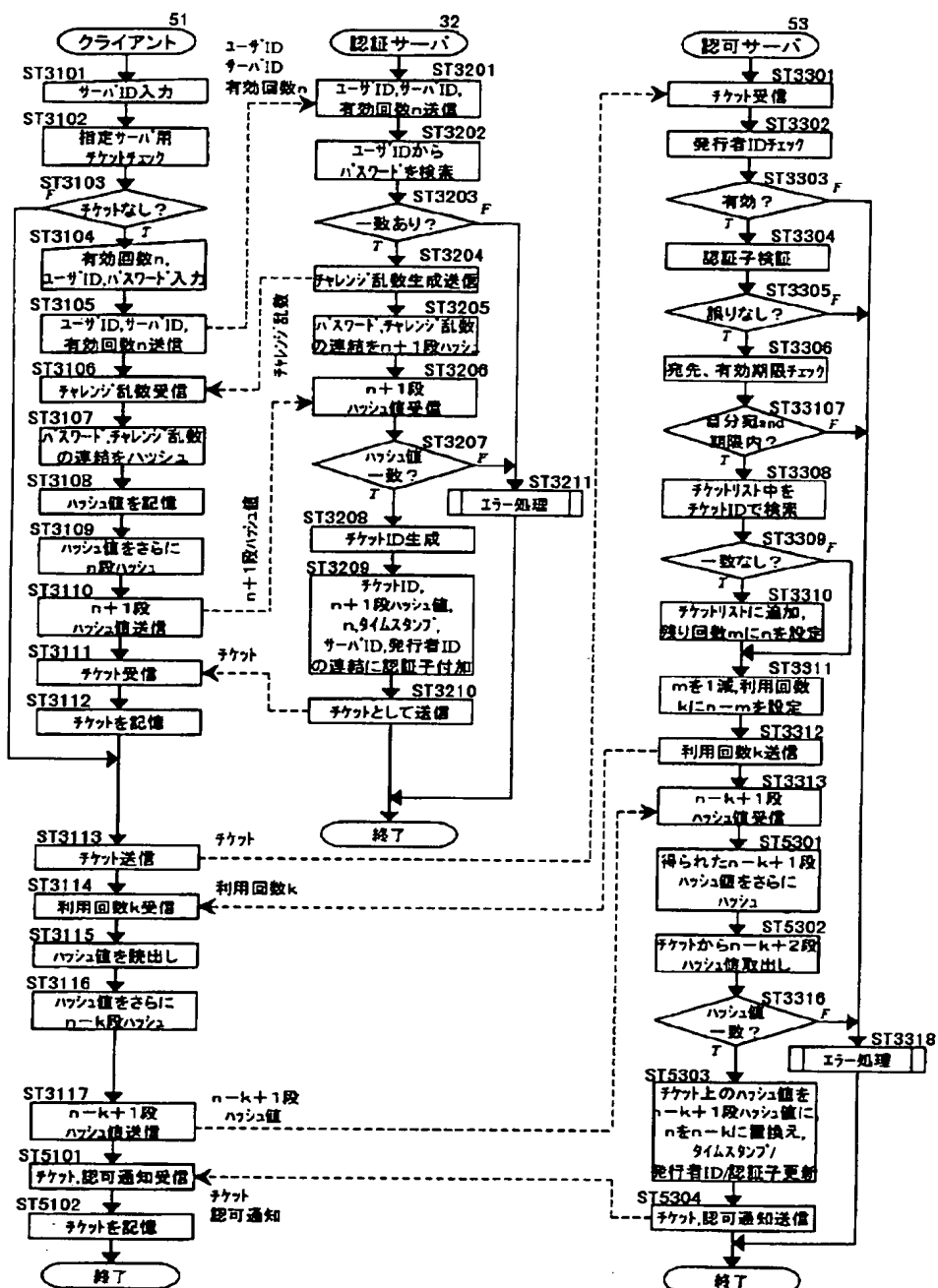
【図17】



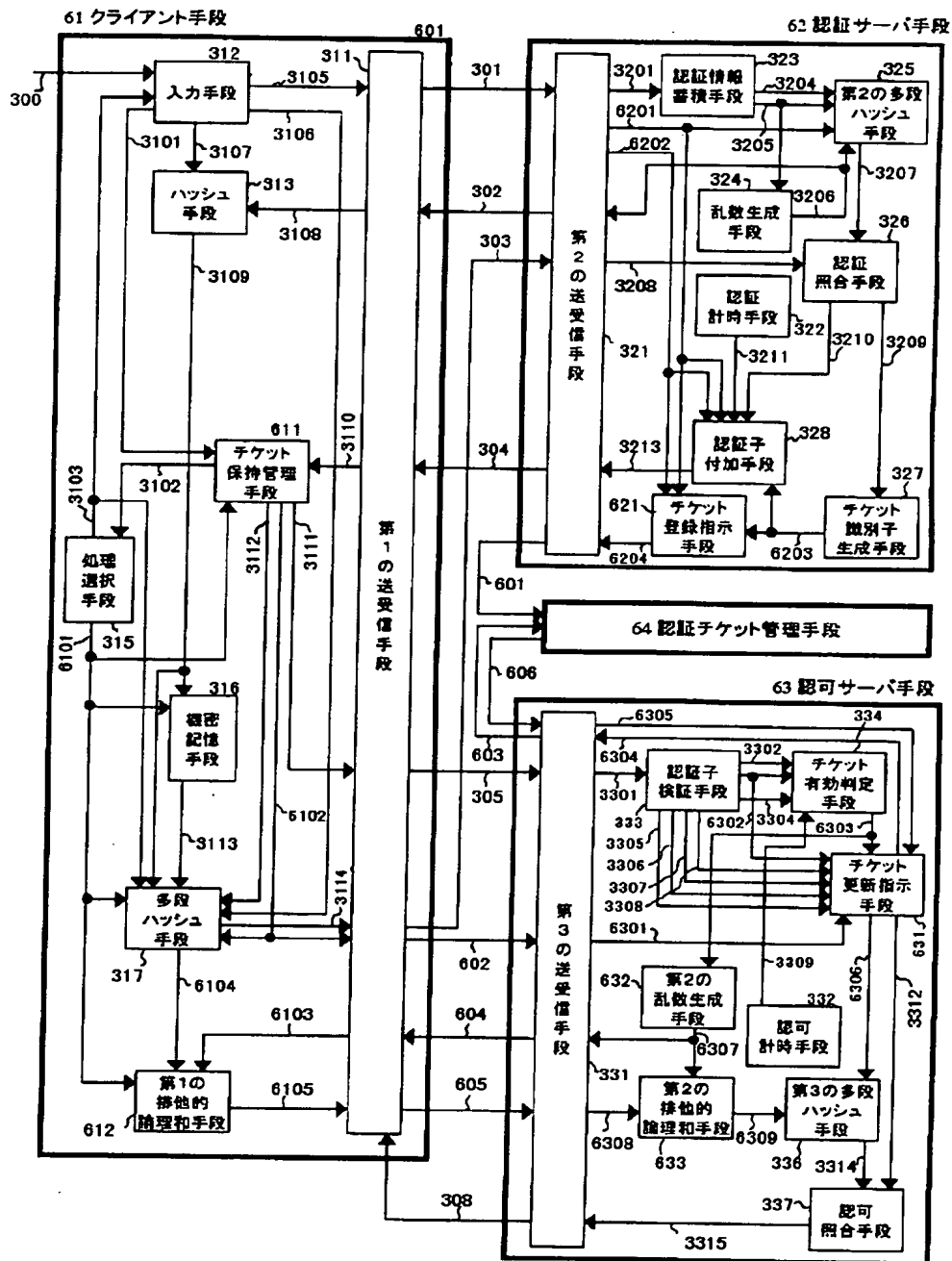
【图 1 5】



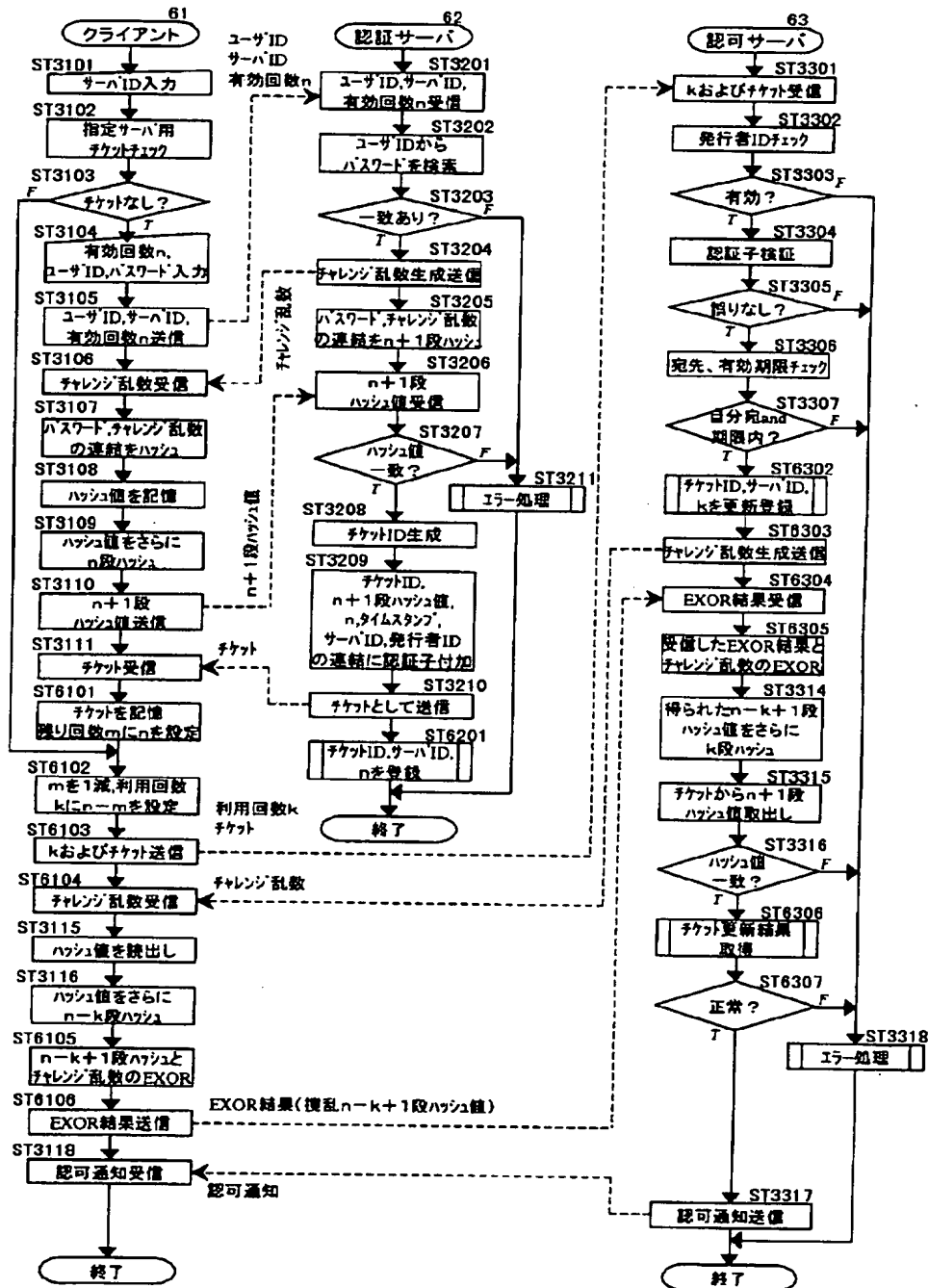
【図16】



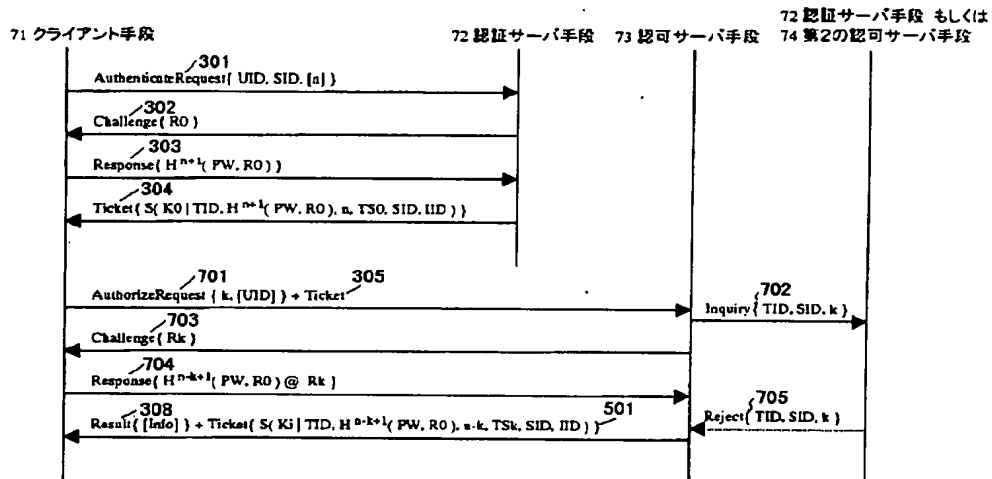
【図18】



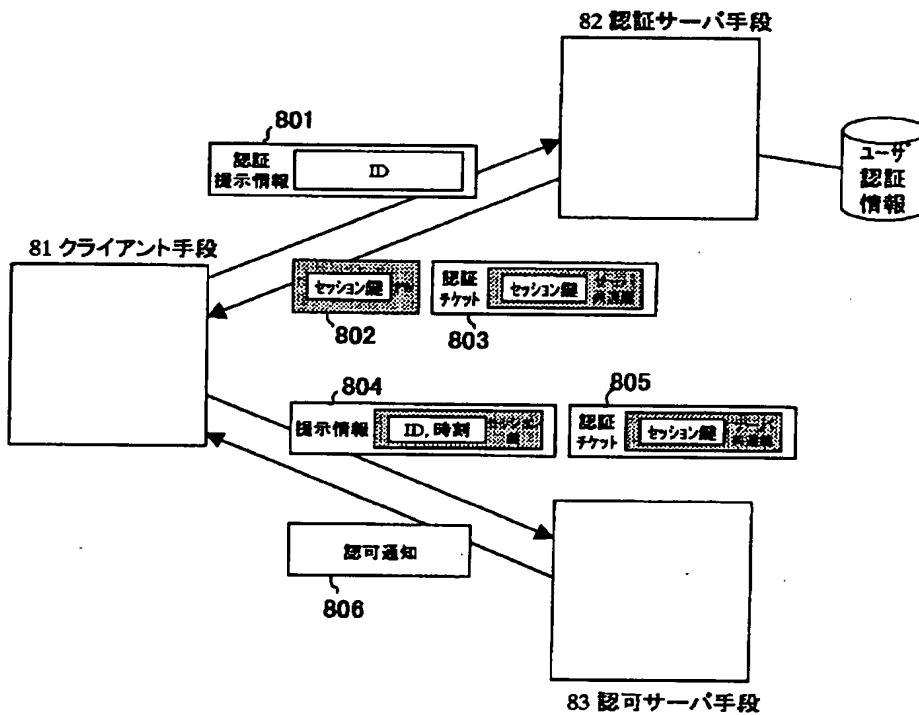
【図 19】



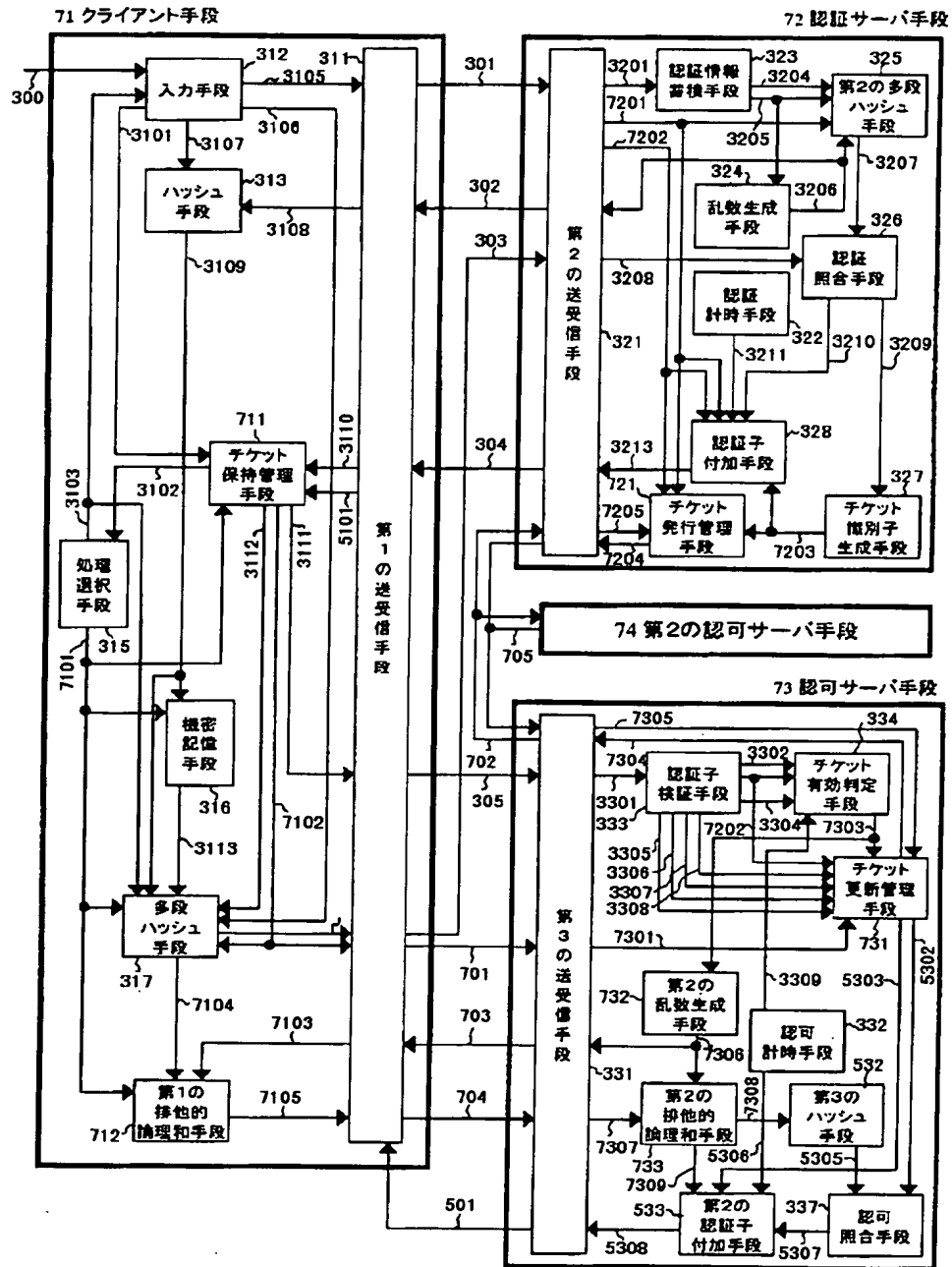
【図20】



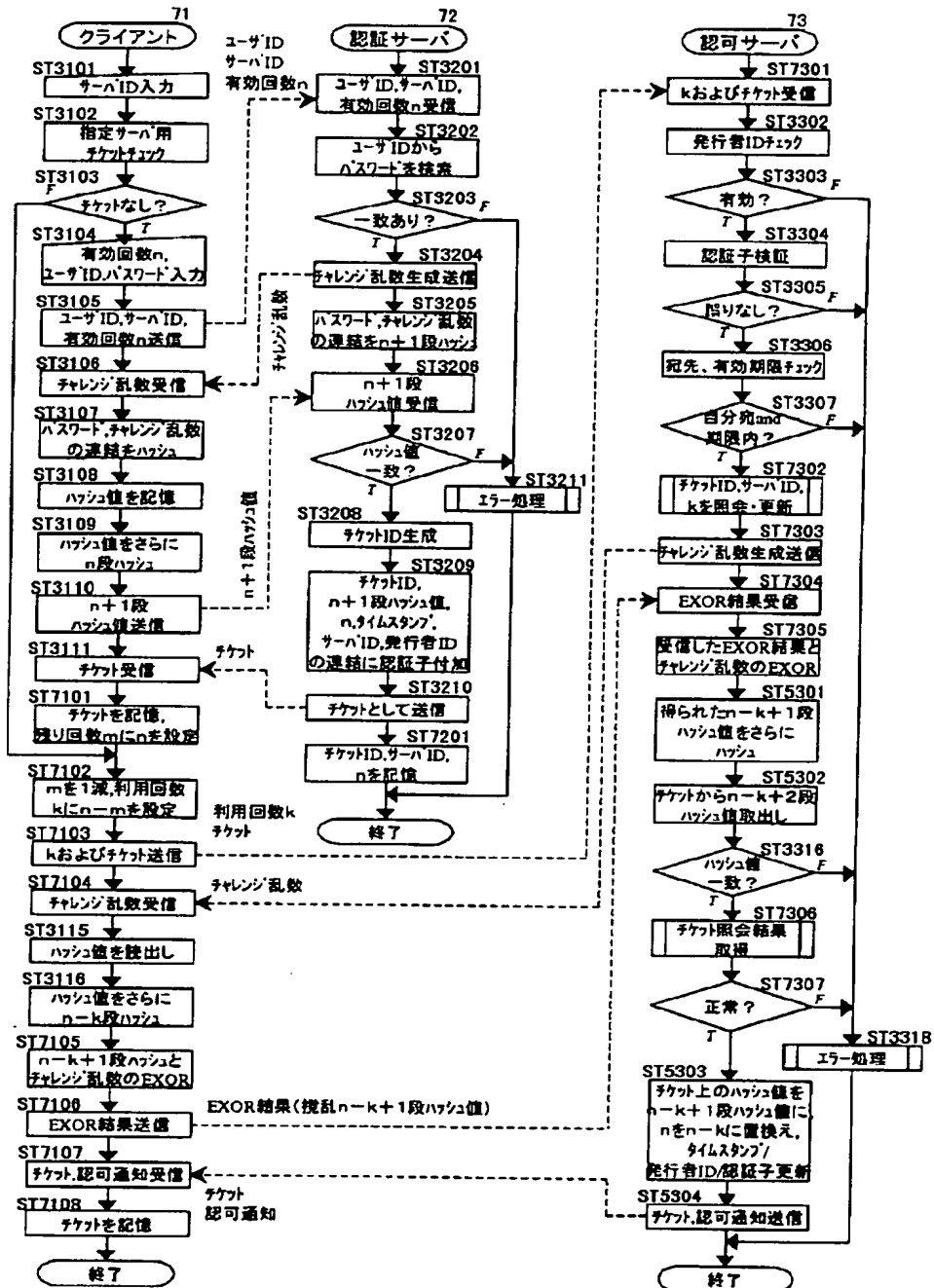
【図23】



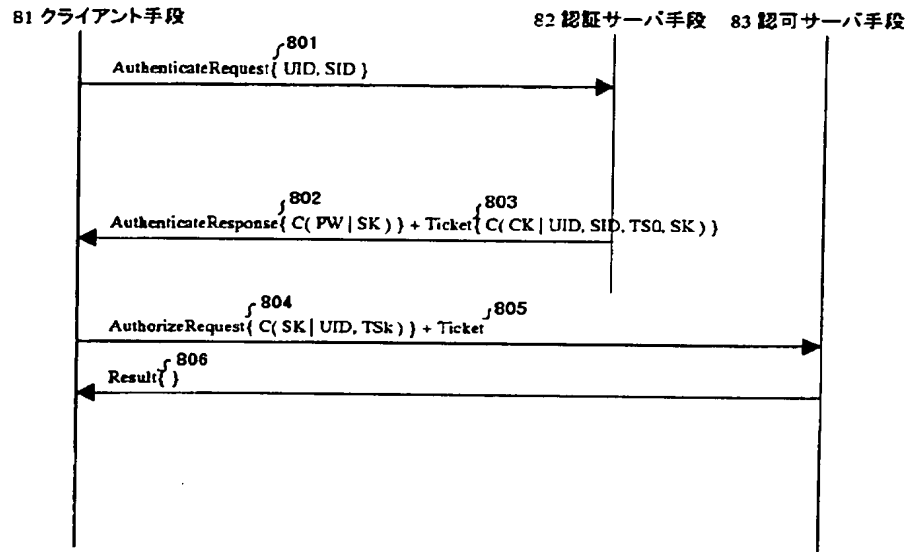
【図21】



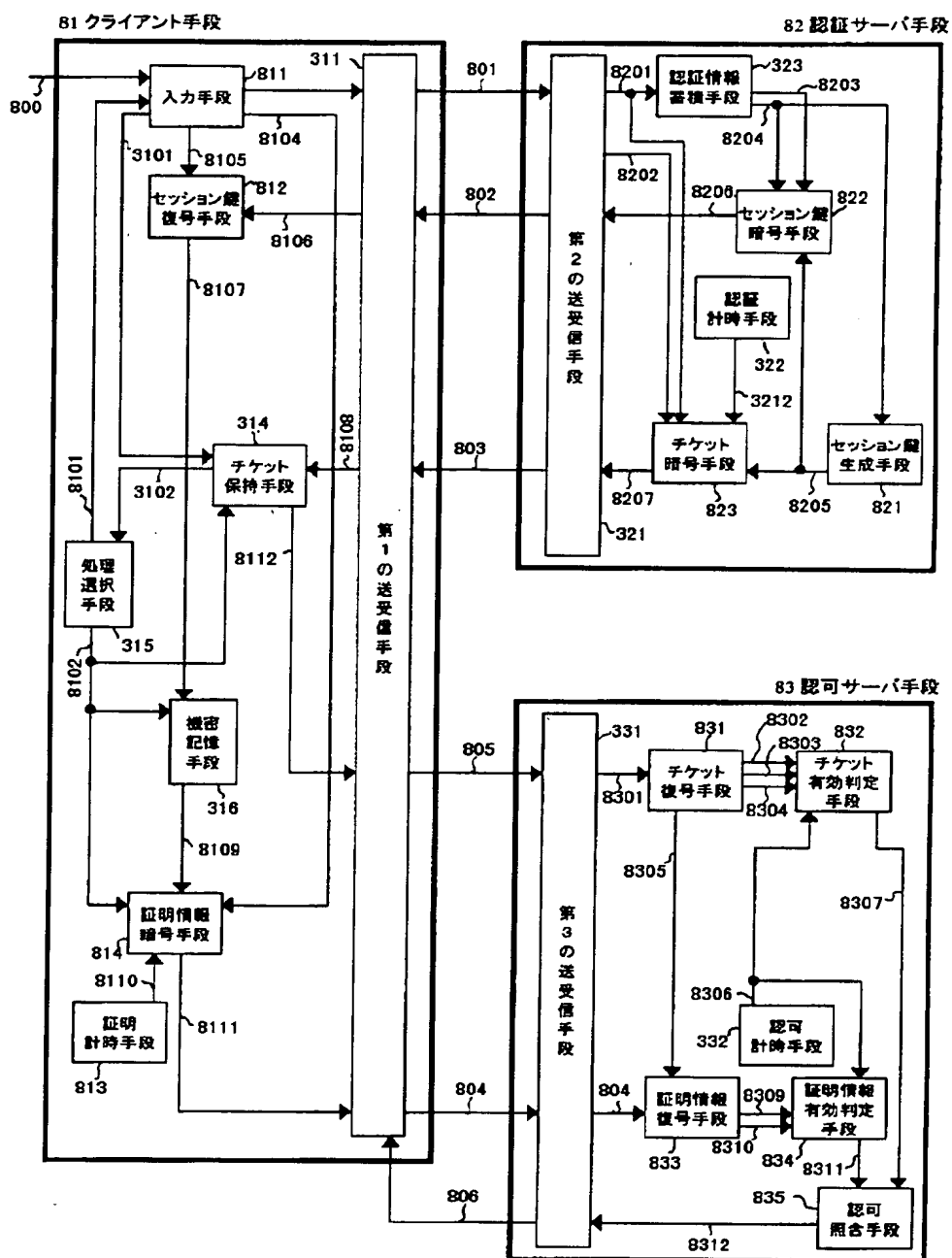
【図22】



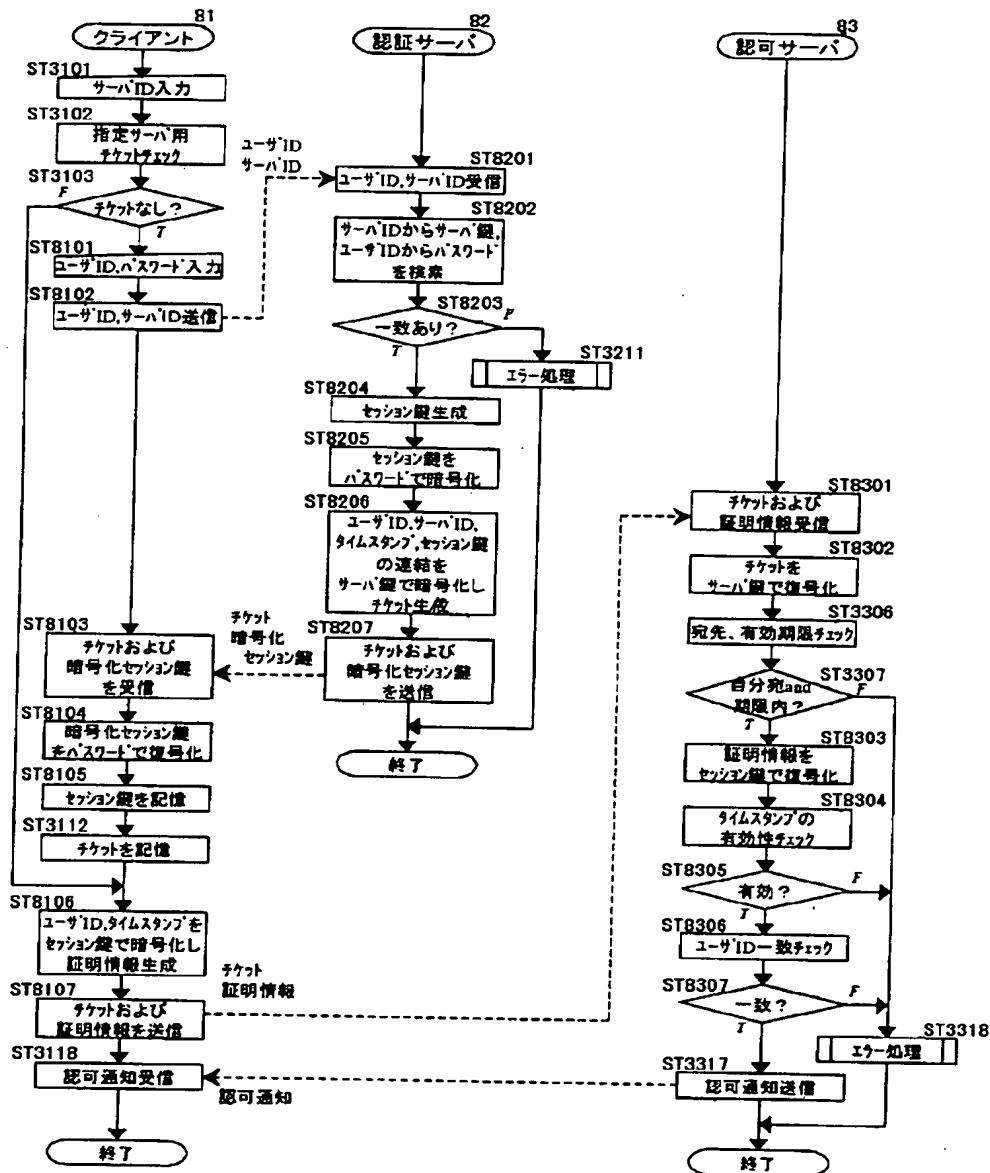
【図24】



【图 25】



【図26】



【手続補正書】

【提出日】平成11年2月2日（1999. 2. 2）

【手続補正1】

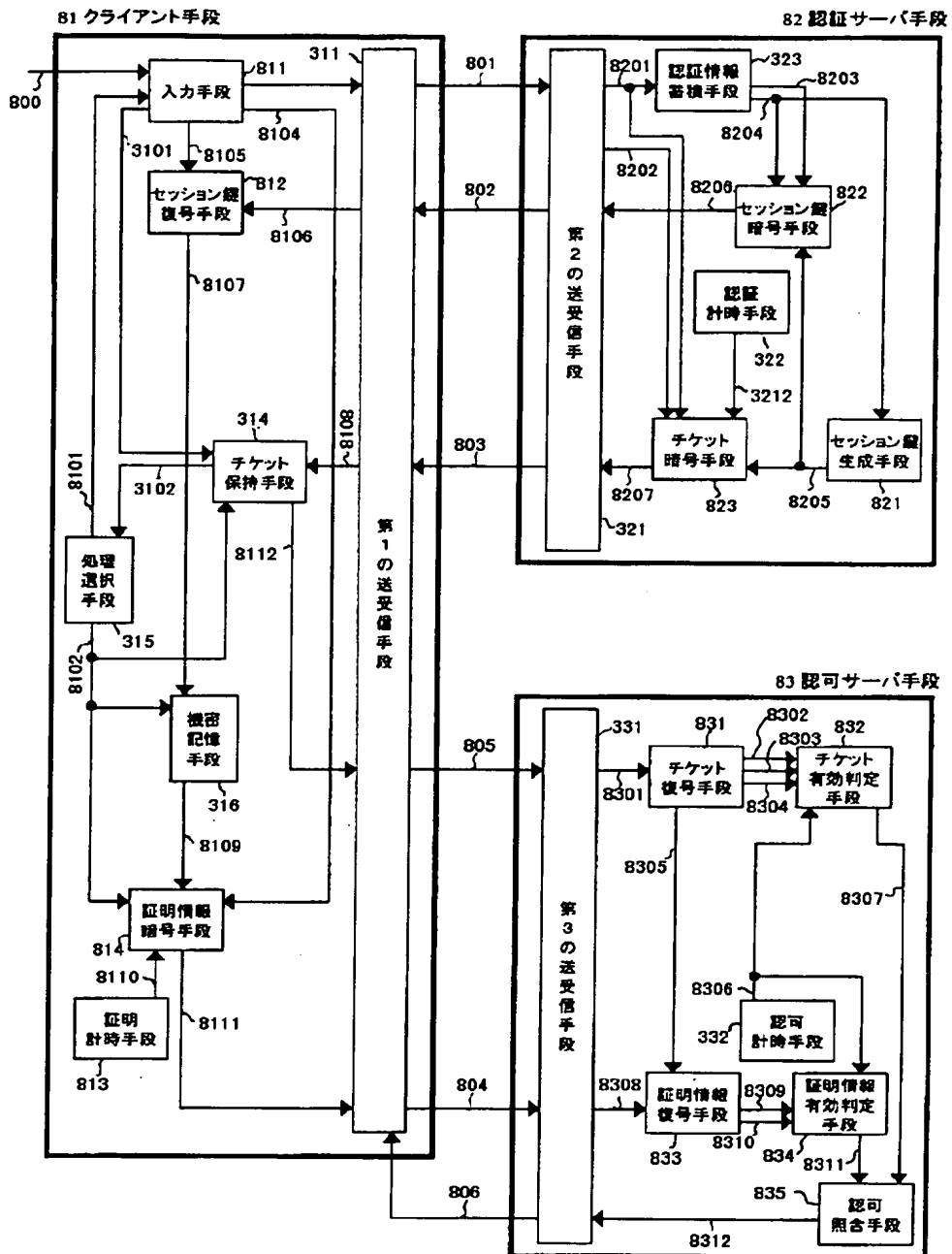
【補正対象書類名】図面

【補正対象項目名】図25

【補正方法】変更

【補正内容】

【図25】



フロントページの続き

F ターム(参考) 5B017 AA01 AA07 BA05 BA07 BB03
BB07 BB10 CA16
5B058 KA33 KA40
5B085 AE01 AE06 AE09 AE13 AE23
BC01 BG07
5B089 GA11 GA21 GB03 KA17 KB13
KC58
5J104 AA07 KA01 KA04 PA07